A Handbook for the Practice of Cyber Diplomacy

Edited by

Andrea Salvi, Heli Tiirmaa-Klaar, and James Andrew Lewis

Print
ISBN 978-92-9462-513-7
CATALOGUE NUMBER
QN-01-25-071-EN-N
DOI 10.2815/5941680

Online
ISBN 978-92-9462-514-4
CATALOGUE NUMBER
QN-01-25-071-EN-C
DOI 10.2815/2342888

Luxembourg: Publications Office of the European Union, 2026

EU CYBER DIRECT

A Handbook for the Practice of Cyber Diplomacy

Edited by

Andrea Salvi, Heli Tiirmaa-Klaar, and James Andrew Lewis

A Handbook for the Practice of Cyber Diplomacy

The diplomacy of cyberspace, or cyber diplomacy has become part of the diplomatic portfolio of every nation. As international recognition of the challenges stemming from cybersecurity grows, and as cyber issues have increased in international prominence, a series of multilateral and bilateral diplomatic efforts have sought to create common understanding, reduce risk and improve stability. These efforts have produced successes in the UN and other multilateral forums, but much remains to be done. The international landscape is shifting in ways that call for more confidence building and dialogue among states, as well as with the private sector and civil society, indicating a growing demand for diplomatic skills to navigate this fast-evolving area.

Cybersecurity is a relatively recent addition to the field of international security and foreign policy. The first two UN Groups of Governmental Experts (GGEs) on cyber issues often saw member states send technical specialists or academics. By the GGE in 2015–2017, leading nations recognised the importance of sending experts with diplomatic and negotiating skills if there was to be progress in creating a common understanding of responsible state behaviour in cyberspace. The need for those who are knowledgeable in the art of

diplomacy as it applies to cyberspace has only grown with the difficulty of the task.

This book aims to provide a practical primer for future diplomats on what is still, despite real progress, a young field of international relations. It will supply foundational understandings for new generations of cyber diplomats, with an emphasis on the art of diplomacy rather than on 'cyber' per se or international relations theory.

To do this, the editors commissioned essays by practitioners and experts on cyber diplomacy.

While accounts may change as the negotiating record becomes clearer, these essays offer an immediate examination of the state of cyber diplomacy and where it needs to go as nations take forward the work on the framework for responsible state behaviour in cyberspace.

Contents

Forewords

Kaja Kallas

In a rapidly evolving digital environment, cyberspace has become an important arena in our daily lives, where the boundaries between public and private domains are blurred, and which is in equal parts risk and reward. Adding to the complexity is the fact that cyberspace is a truly global domain, where data flows seamlessly across national borders. Cyberspace is therefore increasingly tricky for diplomats to navigate. This textbook sets out the basic principles at stake, with essays that explore how various cyber policies have shaped this intricate landscape, evaluate interactions between states and other actors, and examine existing diplomatic strategies seeking to foster a more stable and secure digital environment.

All actors operating in cyberspace are bound by the obligations set out in the United Nations Charter. When Estonia held the Presidency of the UN Security Council in June 2021, in the midst of the COVID-19 pandemic, as Prime Minister I chaired the first high-level open meeting on cybersecurity in its history. This was online, as everything was at that time. I underlined the immense opportunities that digitalisation had presented the country with, including 2-3% savings of the country's GDP every year from taking government services online. I also petitioned for raising awareness of the dark side to rapid digitalisation. As I

said then – and it is still true today – our digital future can only be secured if we follow common rules of the road.

Established legal principles, including the prohibition of force, the right of self-defence and respect for sovereignty, equally apply in cyberspace. Globally agreed norms are also extremely important, as is working together with like-minded partners, recognising the existence of technologically less advanced states where there is a risk of becoming safe havens for cyber criminals and proxy groups, and ensuring accountability for the violation of international law or cyber norms. Governments must also tackle cyber threats together with the private sector, civil society, and academia. Companies have an important part to play by investing into cybersecurity and eliminating vulnerabilities.

The EU's own Cybersecurity Strategy is based on four areas of diplomatic work: 1. Leadership on international norms and standards; 2. Preventing, deterring, and responding to cyber-attacks; 3. Building partnerships and international cooperation; 4. External cyber capacity building. This work is underpinned by the EU's dedication to a global, open, free, stable and secure cyberspace, where international law and norms guide behaviour. The 2024 declaration by the EU and its Member States on a common understanding of application of international law to cyberspace is the most recent testimony to this. Since 2017, the EU has coordinated responses to malicious cyber activity and is continuously pushing for more information-sharing at the EU level. This is particularly important in the current context, where Europe faces persistent hybrid- and cyber-attacks. The EU has also developed an

extensive network of global partnerships and works with its partners across the globe, including international organisations. Via EU-led initiatives including Global Action on Cybercrime, EU CyberNet and EU Cyber Direct, the EU helps neighbouring regions, Africa, Latin America and Asia to improve their cyber security capacities. In my role as HR/VP, I am committed to pursuing an equally collaborative approach to cyber diplomacy during my mandate.

Whether you are a diplomat working for the European Union or for your national government, this is an important reference guide for current thinking in the area of cyber diplomacy and should help you in your daily work. Regardless of where your allegiances lie, cyberspace is a universally accessible and used domain that calls out for universally agreed principles to protect the interests of society as a whole.

Kaja Kallas

High Representative for Foreign Affairs and Security Policy and Vice-President of the European Commission

Izumi Nakamitsu

Rapid advances in digital technologies are generating new opportunities to address global challenges, from mitigating climate risks to pandemic prevention. They are also opening new avenues for states to achieve the Sustainable Development Goals, with each advance an opportunity to accelerate progress.

At the same time, increased interconnectedness and digitalisation are posing new challenges, including those related to international peace and security.

The scale, scope and sophistication of malicious activity in cyberspace are on the rise, resulting in both destruction and disruption. Incidents impacting the infrastructure that provides services to the public and is essential to the functioning of society are particularly worrisome.

From a proliferation of distributed denial-of-service attacks to increasingly sophisticated forms of malware, the cyberspace threat landscape continues to evolve at lightning pace. In parallel, mistrust linked to the digital domain is on the rise.

Against this backdrop, efforts to protect the safety and security of cyberspace are more urgent than ever. It has never been more pressing to build trust and advance common understandings to prevent and mitigate the extension of conflict and hostilities in this domain.

Thankfully, as the urgency grows, so does the attention of the international community. Building on more than two decades

of intergovernmental work at the United Nations, States continue to pursue concrete measures to safeguard the peace and security of cyberspace under the auspices of the General Assembly.

These multilateral efforts have evolved over the last twenty-five years in the form of groups of governmental experts and, most recently, fully inclusive open-ended working groups.

Major milestones and achievements of these efforts include affirmation of the applicability of international law, in particular the Charter of the United Nations, to State use of information and communications technologies, the development of a set of voluntary norms of responsible state behaviour in the use of these technologies, as well as a set of confidence-building measures and common principles for capacity-building in this area.

Great strides have been made, but the work is not yet complete. The United Nations remains committed to supporting States in the critical task of safeguarding the peace and security of cyberspace.

In his proposal for a New Agenda for Peace, the United Nations Secretary-General calls for action to prevent extension and escalation of conflict in cyberspace, including to protect human life from malicious cyber activity. In particular, the Secretary-General calls upon states to declare infrastructure essential for public services and to the functioning of society off-limits to malicious cyber activity.

The 2024 United Nations Summit of the Future facilitated the international community to tackle the risks and opportunities

presented by new and emerging technologies with a view to ensuring that the United Nations remains fit for purpose in responding to them.

There can be no substitute for multilateral diplomacy, which is essential to our common goal of ensuring a peaceful and secure cyberspace.

Izumi Nakamitsu

Under-Secretary-General and High Representative for Disarmament Affairs
United Nations

Nathaniel C. Fick

More than a decade ago, investor and entrepreneur Marc Andreessen famously wrote, 'Software is eating the world.' He was right. The digitisation of everything has transformed how we work, learn, communicate, and access products and services ranging from MRIs to music.

Today, technology is eating foreign policy. Tech issues are interwoven into nearly every aspect of our statecraft, spanning issues from arms control to climate change to foreign investment. We need tech diplomacy—and diplomats who understand technology issues—more than ever.

Driving this change is the new reality that technology innovation as a source of national power and influence is foundational, more akin to geography or demography than to GDP or military capacity. In fact, those traditional measures of strength are increasingly downstream of an economy's ability to innovate and collaborate in key technology areas. Moreover, in any contest between states, or more broadly between systems of governance, many issues held dear by so many of us – from ensuring the competitiveness of free markets to strengthening the rule of law, to extending equal treatment to all people – find purchase only if rights-respecting countries prevail in shaping how key technologies are developed, deployed and used in the world.

In short, we who practise technology diplomacy on behalf of the United States seek to have others choose a more equitable and innovative 'operating system' – a technology ecosystem

that is free and open, interoperable, reliable and secure, and that delivers concrete benefits to all people.

At the core of our approach to tech diplomacy is the concept of digital solidarity. No one country or single company can go it alone. Erecting barriers to the free flow of data, for example, or failing to take advantage of global cloud services for the sake of protectionism, demonstrably increases costs, slows innovation and weakens cybersecurity.

Hard decisions are ahead. The lives of citizens in every country will be influenced in profound ways by issues of cybersecurity, digital infrastructure, data privacy and digital trade. Recent history has shown that software developers, business executives and government policymakers have not gotten everything right. Software is too buggy, misinformation and disinformation are rampant, and technology policy too often moves at the speed of government rather than the speed of innovation.

As diplomats, we need to help identify the key issues, bridge the inevitable gaps between domestic and international policies, build coalitions around shared approaches, and then codify those approaches into structures that are strong enough to endure, but also flexible enough to evolve.

We face well-resourced competitors and adversaries who do not share our vision of a rights-respecting digital future. It is imperative that the tools of diplomacy – dialogue, capacity-building, foreign assistance and the like – remain our tools of first resort in managing the challenges we face. Doing so will require a whole generation of tech diplomats. At the US

Department of State, we train cyber and digital experts with three guidelines in mind, as follows.

First, don't be intimidated. We're not trying to train software engineers or data scientists. We need our diplomats to be diplomats … but with an understanding of technology, an appreciation for its centrality in our foreign policy, and a willingness to lead in the international tech space.

Second, speed matters. Policy relevance on tech topics requires us to move at the speed of technology, at the speed of the private sector, and at the speed of our adversaries … not at the traditional speed of government institutions. Tech diplomats must have a bias for action, recognising that indecision can become a decision as others move ahead without us.

Third, be a champion for solidarity in the digital domain. Ben Franklin said it best during the American Revolution: 'We must all hang together, or, most assuredly, we shall all hang separately.' Nothing generates advantage in the tech domain as much as working together with partners and allies to provide mutual support and help build capacity.

Technology is shaping the most consequential issues in our foreign policy today, from winning the war in Ukraine to managing competition with China, from defending human rights in the digital age to shaping the governance of artificial intelligence.

Diplomacy is most important when it is most challenging. The work of today's technology diplomats—and the policymakers, business executives and civil society leaders alongside them—

will shape the global technology ecosystem for decades to come.

I wish you the best on this journey.

Nathaniel C. Fick

Ambassador at Large
Cyberspace & Digital Policy
US Department of State

Jürg Lauber

Information and communications technology (ICT) comes with a wide range of opportunities and risks for humanity. In addition to other measures, regulation is needed to promote the former and contain the latter: not least in the context of peace and security, and especially at international level.

ICT also poses particular challenges for diplomacy. New means of communication and meeting platforms provide easier access to information, speed up reporting and promise wider participation and increased transparency. But there are disadvantages. Social media can accelerate the spread of misinformation. Virtual meetings offer little room for human interaction and informal exchange, where the real diplomacy happens. The digital divide reinforces exclusivity rather than inclusivity. In addition, the complexity of ICT, whose development is forever accelerating, places special demands on the diplomats who are supposed to regulate these technologies. Incidentally, ICT is developed and marketed by globally active companies whose economic power exceeds that of many countries.

Have diplomats and intergovernmental negotiations become obsolete when it comes to ICT?

I don't think so.

As in numerous other and similarly complex areas, the fundamental challenges remain the same: in the face of new phenomena that impact societies across national boundaries, we need ways to mitigate risks and enhance opportunities.

Especially where promising solutions have a normative dimension, states (and their agents) remain indispensable actors. In order to be sustainably effective, such solutions and norms must be supported by as many states as possible.

The United Nations, including the existing specialised agencies and associated processes, enjoys strong legitimacy as a normative body in the field of technology due to its expertise and quasi-universal membership. It provides suitable platforms for regulations that are intended to have a global reach, such as regarding the use of ICT in the context of international security. However, the peculiarities of ICT favour a so-called multistakeholder approach, i.e. the extension of the traditional intergovernmental framework through the participation of relevant actors from science, industry and civil society. By selecting suitable formats, it is perfectly possible to bring the necessary technical expertise of non-state actors to the diplomatic negotiations while still respecting the intergovernmental nature of a norm-setting process.

Diplomats have the necessary methods to develop a shared understanding and find common ground despite initial divergences, regardless of the complexity of the matter. In addition, multilateral diplomats usually deal with a wide range of issues. They are in a position to recognise interdependencies, assess the impact of specific proposed solutions on other issues and avoid unintended negative side-effects. Nevertheless, as already mentioned, it is essential to provide diplomats with regular access to external experts as part of a multistakeholder approach.

If we want to put scientific breakthroughs and new technologies at the service of humanity and achieve collective progress in the spirit of the 2030 Agenda for Sustainable Development, we need normative frameworks whose legitimacy is guaranteed by broad participation in their drafting and tangible positive impact after adoption. Diplomacy remains an essential craft to achieve these ambitious goals. Multilateralism matters.

Jürg Lauber

The Permanent Representative of Switzerland to the United Nations Office and the other international organisations in Geneva

David Koh

Many small and developing states, including Singapore, see cybersecurity as a key economic enabler in addition to its importance as a national security imperative. A secure, stable, trusted, open and interoperable cyberspace is crucial for all states to reap the benefits of the digital economy, achieve Sustainable Development Goals and raise living standards.

The active participation of small and developing states in the current UN Open-Ended Working Group on Security of and in the use of ICTs (2021–2025), and their strong support for the successful adoption of consensus annual progress reports despite strong geopolitical headwinds, reflect this emphasis. Their support for the inclusion of practical measures to foster confidence building and capacity building in the annual progress reports in addition to the adoption of rules, norms and principles of states' behaviour in cyberspace is reflective of the importance placed by these states on the developmental aspects of cybersecurity.

The transboundary nature of cyber requires all states to cooperate to advance the adoption of a multilateral system of voluntary rules, norms, principles and coordinated capacity building. Cyber diplomacy is no longer a luxury but an urgent need. For cyber diplomacy to be effective and meaningful, states will need to continue to strengthen multilateralism so that the voices of all states can be heard and included. At the same time, discussions should remain flexible and nimble to effectively address emerging threats such as ransomware, while

focusing on practical and concrete measures to foster the security and stability of cyberspace.

Singapore is a strong advocate of the rules-based multilateral order, including in cyberspace. Singapore has been actively engaging our partners bilaterally, regionally and multilaterally to advance cooperation, dialogue and capacity building. The annual Singapore International Cyber Week (SICW) held in October continues to be an open and inclusive platform complementary to UN and other international cyber mechanisms to discuss policy, operational, technical and diplomatic developments.

The Association of Southeast Asian Nations (ASEAN) Ministerial Conference on Cybersecurity (AMCC), which Singapore hosts on the sidelines of the SICW, continues to be a key complementary platform to existing ASEAN efforts for the development and coordination of regional cybersecurity policy and cooperation. In 2018, the 3rd AMCC agreed to subscribe in principle to the UN 11 voluntary and non-binding norms of responsible state behaviour, making ASEAN the first region in the world to do so. This led to the development of a regional ASEAN norms implementation checklist to be finalised in 2024.

Cyber capacity-building programmes run out of the $23 million ASEAN–Singapore Cybersecurity Centre of Excellence (ASCCE), in partnership with a broad range of international governmental and non-governmental partners and academia, continue to provide cyber policy, operational, technical and diplomatic training to officials from within and outside the ASEAN region.

We are only as strong as our weakest link. All states must come together to ensure the success of global cybersecurity initiatives and maintain international peace and stability. Cyber diplomacy lies at the heart of this. We should capitalise on our strong networks and continue this endeavour together.

David Koh

The Commissioner of Cybersecurity and Chief Executive of the Cyber Security Agency (CSA) of Singapore.

PART 1

AN OVERVIEW OF CYBER DIPLOMACY

The Practice of Cyber Diplomacy

James A. Lewis

The environment for cyber diplomacy is shaped by powerful global forces. Cyber issues are relatively new topics for diplomacy, and cyber diplomacy practice is complicated by many factors: competition among powerful states, the presence of influential commercial interests, the history of its development, its sometimes obscure and complicated technologies and the legal and commercial practices that undergird them, and a lack of clarity over the nature of sovereignty. It is in this ambiguous environment that the diplomat must operate.

The environment for cyber diplomacy is one of difficult politics. Whatever consensus on international order existed after 1990 has ended and we are now in a conflict between powerful blocs of hostile nations. The epicentre of this conflict is between the US and China, but Russia, which has long sought a leading role in cyber diplomacy, also remains an important and influential actor. The international order and institutions created in 1945 face increasing challenges in maintaining stability as the contours of influence and national interests shift. This reflects the rise of new regional powers and the relative decline of European industrial nations.

The economics of cyber diplomacy is crucial. While there is a distrust of markets, digital technologies drive global economic

and social integration in ways that policy finds difficult to shape. This technology has produced unparalleled closeness for states and societies, providing both new opportunities and new tensions. The task of diplomacy is to manage these trends to advance the interests of the state and its citizens.

Cyber diplomacy is complicated by its history. Cybersecurity did not start out as a central issue for international relations. It has strong links to espionage, which at first made it somewhat off limits and left countries reluctant to discuss it. It was not initially important for economies or trade. Cyber diplomacy is, at most, less than two decades old, making it an edifice still under construction. That said, the issues that confront cyber diplomacy are not greatly different from other issues in international relations. The same political and economic forces apply to cyberspace. Technology shapes both problems and solutions, just as in nonproliferation, arms control or trade, but does so within the context of the larger political relationships. There are new actors and areas of ambiguity, but the cyber problem is neither sui generis nor subject to such rapid change that diplomacy is impossible.

The initial ideology of the internet, which still retains influence, was that states had a lesser role in cyberspace. Sovereignty would be eroded by technology and force would no longer be used to settle disputes. Some of this reflects 1990s millennial optimism that the end of the Cold War was also the end of history and a new era of international relations had begun. This was wildly optimistic and unfortunately wrong. Sovereignty and state authority were not so much eroded as reshaped, and one of the tasks for cyber diplomacy is guide this reshaping, to

redefine how sovereignty and the state practices developed around it apply in this new and evolving international arena. A key task is to determine how state practice, including international law and a state's international commitments, can be applied in cyberspace, how state practice might be modified, and where new practices are needed.

Diplomacy is an art. Diplomacy's primary goal is to advance the interests of the state that the diplomat serves, through representation, engagement and negotiation, and by shaping public opinion. There are textbooks on diplomacy and on negotiation, sometimes embellished with theory, but the best method is to learn from experience, by watching more seasoned diplomats in action and by participating in discussions and negotiations. Cyber diplomacy involves representing and advancing the interests of the state one represents, not just for cyberspace but for the larger security, economic and political interests of the nation as they shape and are affected by cyberspace and by digital technologies.

What knowledge and skills does the diplomat need? It is easy to overvalue technical knowledge. In the negotiations for the 2013 UN Group of Government experts, when cyber diplomacy was still new, some Western countries sent technologies and technical experts to negotiate. In contrast, Russia sent a highly experienced diplomat schooled in the strategic arms control negotiations of the 1980s. At one point, the Russian negotiator was even able to get Western technical experts present as negotiators to disagree with their own countries' position—an astounding act of diplomatic bravura.

At least for negotiations, if the choice is between technologists with little diplomatic experience and diplomats with little technical knowledge, the latter is preferable (in this case, the Russian combined diplomatic skill and adequate technical knowledge) and more likely to result in positive outcomes. If a country can afford to send an accompanying delegation of experts (technical and legal) to support its lead diplomat, that can be best, but in most circumstances they should not lead. There is still some contention about the value of technical expertise, but it is largely driven by debate over the role of civil society in diplomacy: both the role it would like for itself and the role it can effectively play.

Civil society

Cyber diplomacy goes beyond the conventional margins of diplomacy. It involves non-state actors that include corporations and 'civil society,' a community linked to academia (in fact, much of civil society could be regarded as a politicised academia), usually of Western origin and often influential in democratic states. The inception of civil society came from a sense of possession by those who first developed and operated the internet: that they alone had the needed expertise in an environment where, in the millennial views of the 1990s, states were becoming less important. This pioneering view was steadily undercut as the internet moved to become a crucial global infrastructure, a move that created security and political issues that few states could ignore or were willing to entrust to others.

Internet culture is vibrant and energetic, but not always well-informed. This complicates the task of cyber diplomacy, since many initiatives will be announced by civil society or corporations yet will have no real effect on the actions of states. State policy must take these initiatives into account and assess the likelihood and timeline for effect (and diplomats can seek to exploit them). No state will allow its interests to be safeguarded by technicians, executives, lawyers or academics, and the steady change in cyber diplomacy over the past two decades has been to move civil society and technology companies from a central to a supporting role in cyberspace. Their roles remain important, even essential, but the new emerging regional powers – China, India, Brazil, Turkey, Nigeria, Indonesia and others—will not defer to them. These states are the voices that will reshape international relations and perhaps modify the norms and practices inherited from the twentieth century. There is some dissatisfaction among the new powers with the international institutions assembled after the Second World War and their transatlantic focus, and this includes the deference shown to private actors by some 'like-minded' states.

The fact that the big tech companies are usually American also creates a degree of unhappiness (even among allies). A related issue (not always recognised) that shapes cyber diplomacy is the awkwardness in relations between former colonial powers and their ex-colonies. This awkwardness need not be determinative but must be taken into account. Change does not require a wholesale scrapping of the existing system, but its modernisation to reflect the new global polity. Both cyber diplomacy and emerging technologies will play a central role in this modernisation.

For companies, cyber diplomacy is often an extension of the lobbying practices they use with national governments, to persuade officials to undertake an action that serves the company's interests. Civil society participation is more complicated. In some instances, groups can assert that they better represent the interests of the citizens than the formal representative of the state. In other instances, they can strongly advocate for a single measure to the exclusion of others, whereas a diplomat needs to balance multiple and competing measures. Civil society groups are largely a Western phenomenon and while this increases their political salience in Western capitals, it can also undercut their legitimacy with authoritarian or non-Western states. A cyber diplomat should see civil society as a useful adjunct to develop ideas, build support and shape global narratives that support national interests, and one advantage for the democracies is that they have civil societies while their authoritarian opponents do not.

The role of these informal diplomats remains a point of contention even in democratic societies, where citizens are free to challenge policy and assert alternative views. For the practitioner, it is worthwhile to listen to and consider these alternative views, if only because they can offer valuable insights and contributions. This must be accompanied by a frank assessment of the practicality of any suggestion. Calling for a Cyber Geneva Convention, for example, faces insurmountable obstacles. At the same time, at least one set of parties in this conflict among states is unwilling to make concessions. Whether this is right or wrong is less important than the recognition that this is the political terrain for diplomacy, on which the cyber diplomat must operate if the

goal is to defend and advance the interests of their state. Diplomacy is clearly no longer a task only for diplomats (e.g. those who represent states) but the formal representatives of national governments are the most important voices, because only states can commit a nation to a binding agreement or legitimately use force and violence. The task for diplomats is to ensure that these unofficial efforts support their national goals rather than undercut them.

National strategies for cyber diplomacy

In the past decade, a majority of countries have issued national cyber strategies, some of which are even in their second iteration. Diplomacy can be part of a larger discussion of economic, security and societal goals, or it can be a stand-alone strategy. Well-written strategies set goals, assign responsibilities and help ensure a coordinated national approach among national agencies and with multilateral organisations like the Organization of American States (OAS), Organization for Security and Co-operation in Europe (OSCE), Association of Southeast Asian Nations (ASEAN) and the African Union, which play a central role in cyber diplomacy (these are discussed in separate essays in this volume). Strategies are only as good as their implementation, but even the act of developing a strategy can help clarify thinking and organisation and articulate national interests in cyberspace.

A national strategy as a public document is also an important tool for communicating national views and intentions to other countries, to civil society and to a national audience. This makes

the drafting and presentation of such strategies an important diplomatic tool. While the public value of a strategy declines as it ages, it will serve as a reference document and, in varying degrees, a commitment to the direction cyber policy will take. The struggle in drafting a national strategy is finding a balance between platitudinous assertions and concrete actions, and in deciding how public to make any plans for action. Few expect a national strategy to be a wholly binding commitment, but many will scrutinise it for indications of interests and intent.

A diplomatic strategy also provides a vehicle to consider how to integrate the international challenges presented by emerging technologies. The strong interest in artificial intelligence (AI) guidelines and norms in some way reflects the earlier experience and successes of cyber diplomacy. These guidelines and norms for technology will continue to evolve as technologies mature and as actual problems they create for international relations become clear. Like cyber issues, there are some useful precedents for emerging technologies that can be drawn from earlier security and trade discussions, but these are not aways applicable. The topics are new enough (in diplomatic terms) that no precedent is perfect, and any precedent must be applied carefully and with adjustments.

For example, the Geneva Conventions and the IAEA are often cited as precedent for emerging technologies, but they are at this point of limited value. The Geneva Convention grew out of actual experience that pointed to real problems in the conduct of armed conflict. Hypothetical concerns not support by experience do not command the same weight and may not be enough for meaningful, binding, agreement among powerful

states. Similarly, the International Atomic Energy Agency (IAEA) is based on a formal, binding treaty that has broad international support and relatively easy verification of compliance (based on a global network of sensors and the national technical means of a few states). There is no equivalent for cybersecurity. Strategies can identify patterns and usefully develop the approaches for applying them to cyber and emerging technologies, but it would require considerable diplomatic effort accompanied by actual experience for the Geneva Conventions and the IAEA to become useful precedents.

Current discussions are based on predictions of the course new technologies will take and the problems this will create. Many of these predictions will be wrong. The challenge for diplomats lies in developing the sources (often in business and academia) that will let them better assess and predict the direction technology will take. This means getting out of the embassy and talking to more than the foreign ministry, something that resources and interest may not always support, but a number of countries have created 'tech envoys' whose mandate goes beyond cyber or have expanded the reporting and representation functions of the embassy to address this.

International law

As with technical expertise, it is easy to overvalue legal knowledge in cyber diplomacy. One of the authors of the *Tallinn Manual* once remarked that if only the diplomats would get out of the way and let the lawyers handle things, the cybersecurity problem could be solved in a week. This is hubris

and the counterpoint is the Draft Articles on State Responsibility for Wrongful Acts (2021), prepared by the UN's International Law Commission, and in draft now for more than 20 years because even if lawyers can agree, states will not, if their core interests are in conflict. State practice and sovereign concerns usually take precedence over international law.

One reason for the imprecisions and lack of exact definition in many treaties (which are not like legal contracts among businesses) is that negotiators have sought to preserve the discretion afforded to states in decision-making. As one negotiator put it, they did not want specific definitions because they wished to preserve the flexibility and discretion enjoyed by their political masters. The greater the implications for sovereign rights, the more cautious states will be in reaching agreement, and one skill needed for diplomacy is the ability to use constructive ambiguity: phrases acceptable to all parties, open to later interpretation, and sufficient at the moment to provide both agreement and a degree of understanding on how states will behave.

There are, unsurprisingly, varying views among countries on the applicability of international law in cyberspace—for example, members of the European Union are more likely to be guided by international law as a cornerstone in their approach to foreign affairs. Smaller states also will prefer an emphasis on international law in the hope this provides a degree of restraint on more powerful neighbours (and in cyberspace everyone is, in some degree, a neighbour). Frankly, this preference for law on the part of many states creates an opportunity for persuasion that diplomats can use to win support for their

proposals, if they can find a balance between protecting sovereign rights and acceding to (or acknowledging) universal principles. The applicability of international law is also part of a larger disagreement among states over universal commitments (which some countries describe as 'Western' rather than universal) and sovereign rights. The less democratic a state, the more likely it is to object to universal obligations as they conflict with the older concept of sovereignty, which gave each state unimpeded rights over its internal affairs and how it treats its citizens.

While no nation will say that it does not abide by international law, state practice can take a different course. Smaller states can prefer a legalistic approach to diplomacy as it provides them with a degree of protection and influence, but great powers will take a more flexible view of international law, particularly in issues where they are in conflict (even if it is not armed conflict). Diplomatic experience would show that appeals to law or appeals to reason are not always effective. Law is only one factor in diplomatic relations and not usually the primary factor. Power and self-interest play the central role in states' decisions, uneasily balanced against normative commitments. A key task for diplomats is to understand the assumptions that guide the thinking of those with whom they will interact or negotiate, and who may have a different logic and values. The strongest diplomats and negotiators tailor their approaches to consider the other parties' interests, culture and priorities, which will outweigh the application of international law.

Sovereignty

Sovereignty is a foundational concept for diplomacy. The globalisation that began in 1990 has ended, in part because whatever economic and technological forces drove it, most states were unwilling to see their sovereignty diminished by some amorphous and impersonal force. The return of sovereignty, often in the form of opposition to a global order shaped by American values in which the United States was often predominant, complicates the diplomatic landscape by introducing new forces and interests. The resurgence of sovereignty dilutes the effect of appeals to universal rules or international laws and calls for a recalculation of both how to best advance national interests and what those interests are.

The evolution of sovereignty, driven in good measure by technological change, is a fundamental problem for diplomacy. The technology of the internet operates at immense speed and can give the illusion the there are no borders. In fact, every element of cyberspace is subject to national jurisdiction. One way to consider the task of cyber diplomacy is that it is an effort among states to cooperatively extend existing rules and practices that govern international relations among sovereign states to this dynamic environment, such as defining how existing obligations for human rights, conflict and trade apply to the new technologies and where new understandings are needed.

The illusion of a borderless space is accompanied by the reality of porous digital borders—the internet was not designed with sovereignty in mind. This creates unavoidable issues for the

concept of sovereignty, and for relations among states. Since 1945, the traditional concept of sovereignty has been challenged by the argument that there are universal responsibilities identified by the international community that take precedence over the sovereign rights of states. Disagreement over this point, and whether there are universal values at all, will shape cyber diplomacy for the foreseeable future. One fundamental difference among competing blocs is over the rights of a state to act in untrammelled fashion in its own territory (and the precedents for untrammelled treatment by a state of its citizens from the 20th century are concerning, since a state that does not respect its citizens is likely not to respect its international obligations).

The lack of clarity over the application of sovereignty in cyberspace complicates cyber diplomacy. When a tank rolls over a border, the violation of sovereignty is clear and so, in many cases, is the response. The same is not true for an action that takes place on the internet. Concern over attribution (the determination of responsibility) has slowed the creation of accountability for wrong cyber acts. One dilemma is that it is natural for smaller states to attempt to apply the evidentiary threshold used in courts to international relations. This is inappropriate for international relations (why this is so entails a complex discussion of equality among states, where the powerful pay more heed to their interests than to law) and a different approach is required to best serve national interests. In reality, the ability to assemble evidence and attribute the source of a cyber action varies among states and some are quite capable, but concern over misattribution is high and

another task for cyber diplomacy is to build the political framework for collective action to promote accountability.

The tools of diplomacy are persuasion and coercion. There are limits on the use of cyber tools for coercive purposes, the most important being that nuclear armed states or alliances (which includes most of the advanced cyber powers) are reluctant to cross an implicit 'use of force' threshold, the use of force being defined as actions that cause casualties or destruction (if Russian actions in Ukraine are an example, nuclear states are less reluctant to use offensive cyber actions against non-nuclear states). Leading cyber powers seek to manage the risk of escalating conflict while still engaging in coercive and damaging actions while staying below this force threshold, and cyber tools are ideal for this. This threshold means that respect for sovereignty in the current contest is limited when it can be enforced neither by law nor by force. New technologies, such as artificial intelligence and quantum computing, are more likely to accelerate these trends than to reshape them.

Cyberattacks depend on a combination of software, networks and trained personnel. Perhaps fewer than 30 states have these skills, which are a recent addition to state capabilities for the use of force and violence to achieve political objectives. Cyberattacks can disrupt or damage critical services and degrade the performance of weapons and commanders, but such actions are exceptionally infrequent. In contrast, malicious cyber actions are so frequent as to be considered routine, and while most hostile or criminal acts in cyberspace are called attacks and while public accounts routinely exaggerate effect, few if any cyber actions have produced a measurable

degradation of the opponent's military and economic capabilities. Espionage, crime and political interference are the constant background for cyber diplomacy.

The routine disregard for other states' sovereign rights in cyberspace and the difficulty of enforcing sovereign rights can at times make diplomacy appear feckless. Western nations have relied on largely symbolic actions (like targeted sanctions) to protest violations of their sovereignty by hostile states or their proxies, and these have proven ineffective as a remedy. The combination of an aggressive disregard for sovereign rights and the lack of an effective response is one of the primary reasons that cyberspace is unstable and dangerous.

The normal tools for establishing sovereign rights, using diplomatic and at times coercive measures, have not worked in cyberspace. This largely reflects an unwillingness by the victim states to hold their attackers accountable, and the effect of demarches, public objections, even sanctions has declined to the vanishing point. Finding ways to create accountability and reestablish sovereign rights is a primary task for cyber diplomacy. The extension of sovereignty into cyberspace is a political imperative for governments if they are to discharge their responsibilities. This is not an easy task, and will challenge cyber diplomacy for years to come.

Defining responsible state behaviour

The discussion of norms of responsible state behaviour began in 2009. At the start of the 2009–2010 GGE, there was no agreement among the squabbling member states on the

concept of norms, confidence building and capacity building did not appear in the bracketed text of proposed language by the US, China, France, and others. Confronted by dissension, the chair agreed to use the mechanism of a 'chairman's draft', where, instead of attempting to combine the very different submissions from participating states, he would present his own draft reflecting his sense of the previous day's discussions at the start of every morning session. This allowed him to manage the discussion and, subject to the assent of participants and the chair's willingness to amend it in the light of proposed edits that were acceptable to the larger group, prepare a coherent text that ultimately became the final report. Using an iterative drafting process that introduced new ideas presented by members on the floor or by written submissions, the chair developed a text acceptable to all participants.

The introduction of the concepts of norms and confidence-building measures (CBMs) came from precedents found in previous international agreements, such as the Missile Technology Control Regime, which is a voluntary arrangement where members agree to observe norms for the responsible transfer of missile-related technology (Missile Technology Control Regime, MTCR) and Cold War arms control agreements (fortunately, the chair of the 2009–2010 GGE was a veteran of these Cold War arms negotiations). Note that these precedents did not come from UN agreements, but from separate great power agreements. One of the changes in cyber diplomacy is that the older arms-control approach has now been superseded by a broader and still somewhat inchoate approach, but in 2010, arms control was still a useful precedent. A similar process led to the 2013 breakthroughs, again led by a

very effective chair, that saw agreement on the 11 norms of responsible state behaviour in cyberspace.

As essays in this volume make clear, the UN is only one venue for discussion and agreement, and it is not always the most productive. Cyber diplomacy requires an ability to track these regional initiatives, influence those to which one is not a party, and use them in turn to help shape and drive global negotiations in the UN. There can be resource constraints that limit the ability of some states to track other dialogues (this is where drawing on civil society resources can be helpful), but the study of these discussions will repay itself in diplomatic effectiveness.

As an aside, capacity building did not appear in the 2010 chairman's draft until the final few days of negotiation. While the chair was responsible for introducing the ideas of norms and CBMs to the group, it was the delegate from South Africa (the only African country represented), speaking on behalf of the developing world (his phrase), who said he would not give consent unless capacity building was included in the GGE Report. In a consensus-based negotiation, even one state can block agreement, and the chair agreed to add the South African proposal.

The development in 2010 of the diplomatic agenda for cybersecurity (the creation of norms, CBMs and capacity building) coincided and contributed to the change in representation from technical experts to those with diplomatic experience and a knowledge in many cases of international security issues. Ultimately, agreed norms reinforce international law, but legal issues did not figure greatly in the initial GGE

discussions. The GGE experience, in many ways the start of cyber diplomacy, points to practical steps for cyber diplomats.

One such step is ensuring familiarity with the actual texts of existing agreements in relevant or adjacent fields such as security, crime or trade. This can be very helpful in developing agreed language. At a practical level, the reuse of previously agreed text reduces the burden of reaching agreement, since states have already approved it. The language used by the chairs in the series of GGE texts from 2009 to 2015 came from a series of agreements, as well as the suggestions of member states, including the Conventional Forces in Europe (CFE) agreement, the Helsinki Agreement and the MTCR. Reference to other agreements, sometimes in an almost formulaic manner, such as references to Human Rights Council Resolutions, can take difficult issues off the negotiating table and allow for progress.

Another practice that can make reaching agreement easier is focusing and narrowing the scope of discussion by taking things off the table for negotiation. There are intractable issues that cannot be resolved, and there are some topics where disagreement is entrenched. If the objective of the discussion is to reach agreement, it may be better to refer to existing language on the topic, as with human rights, for example. The same is true for terrorism. Since agreed language exists in other UN documents, an astute negotiator will draw upon them to ease the process of reaching agreement. Knowledge of and an ability to draw upon the corpus of agreed language for diplomacy is a crucial skill.

Similarly, the use of ambiguous phrasing is at times necessary to reach agreement. While it may annoy lawyers, there are some subjects on which precise agreement cannot be reached. Ambiguous language allows all sides to agree on a topic and leave open the question of interpretation for later. The UN Charter, for example, does not define 'force' in Article 2/4 or 'armed attack' in Article 51, two articles that are crucial for the understanding of cyber diplomacy, which the drafters of the Charter intentionally left undefined to allow for agreement and to provide room for discretion in national decisions. Not only can diplomacy be gradual, but its language can also be imperfect, as a perfect solution may be one to which states will not agree.

A shifting environment

The unipolar moment that emerged at the end of the Cold War ended in 2001—the attacks of 11 September derailed it. In its place there is an emerging multipolar environment, with the US acting as primus inter pares but incapable of imposing its will in all situations, and competing for influence with other states with different views of sovereignty, the international order and their place in it. This new arrangement has not fully hardened into blocs, and there are disputes and tensions within blocs (between the US and the EU, or between China and Russia), but tensions between the emerging blocs limit the scope for cyber diplomacy. Nor do the blocs fully reflect the international community. Between the blocs, there are many countries, most

in the developing world, that fall in neither camp and will listen to the views of both.

Cyber diplomacy is not sui generis but a part of a larger international realignment driven by both political and technological forces. The ability to create new technologies and take advantage of them is a new source of national power. The linkages between power and technology are complex. At a basic level, a nation's power derives from its economic strength, military capabilities and political influence. Advanced technologies affect each of these elements. The effect can vary among nations, reflecting their culture, acceptance of risk and change, and connections to the global economy. Nor is the situation static. Technological progress is cumulative and continuous and the pace at which nations adopt new technologies will help to determine their power relative to others. The effect of technology on diplomacy goes beyond cybersecurity or traditional arms and trade discussion and is still being defined. Some countries have created 'tech envoys' to monitor commercial and academic centres of technological change and build connections to them.

There are instances where small countries have been able to exercise influence on the international scene that is disproportionate to their size or strength. Conversely, wealthy countries with advanced technologies can find that their power is less than the sum of the parts, especially regarding political influence. New technologies may actually work to diminish a nation's influence. There are now many alternative channels for information and opinion that limit the ability of governments to dominate the public narrative debate. Public diplomacy,

raised by Woodrow Wilson in 1919 and which might be described today as shaping the narrative, is now a central element for international relations and diplomacy that new technologies only complicate.

Precedent is not always useful as a guide, as the international situation continues to change and the shaping trends are neither the unipolar moment that existed from 1990 to 2015 nor the bipolar conflict of the Cold War. This means that precedents must be chosen carefully and, while still useful, may have more limited application both in designing policy and in predicting action. Assessing the likely effect of any national initiative is, like diplomacy itself, something of an art, shaped by the intentions (and actions) and capabilities of other states and actors. One lesson is that most nations' international cyber policies are shaped by their larger approach to international problems. A broader knowledge of a state's foreign policy is necessary to accurately develop cyber policies and assess the probable effect of their actions.

The arc of cyber diplomacy has trended away from consensus and agreement on universal principles. There are at least three camps divided into various regional groupings that shape cyber diplomacy and diplomatic strategy. A group of likeminded Western democracies are challenged by authoritarian states, but most countries find themselves uncomfortably in the middle. While a majority of the countries in the middle favour international law as a pillar of diplomacy, differing views of sovereignty and of national interests in both security and economics create powerful forces that shape their diplomatic actions and require sensitivity and a willingness to listen – a

common trope among these states is their dislike of being lectured by Western countries. A starting place for discussion can be national cybersecurity strategies, which, while often formulaic, can provide insights into national positions. A focus on military security can be unhelpful since the key concern for many countries is economic development, not security, and an approach that emphasises risk rather than growth will not be persuasive.

No one has ever died in a cyberattack, and while a source of economic damage, cyber actions have not been crippling. Offensive use is shaped by several factors, and the very limited success of Russian cyber effort in Ukraine should give pause to catastrophists. Those outside the cyber community may assign cyberattack a lesser importance, and this affects the willingness to agree to binding commitments (like the Geneva Convention or the International Atomic Energy Agency and the Non-Proliferation Treaty). Malicious cyber activity is a growing source of concern and instability but not yet a threat significant enough to compel binding action that meaningfully constrains the actions of states. It would be reasonable, however, to assume this will change for the worse as dependence on technology and cyber infrastructures increases and as relations among great powers deteriorate. Since we can see this as a likely outcome, one task for cyber diplomacy is to prepare and build the structure of agreement needed to minimise harm.

Cyber diplomacy at its core is neither technical nor legal. Like any other diplomatic task, it is political, involving politics among states and among those who represent states. The immediate task is to identify which instruments of international

order can now be applied to cyberspace. This volume aims to prepare future generations of diplomats for what will prove to be a daunting task. At the current time, it may only be possible to reach agreement among likeminded states, and perhaps manage and reduce the chance of conflict between those with opposing views. This, however, is a worthwhile goal for diplomacy.

James Lewis

Pritzker Chair at the Center for Strategic and International Studies

James Lewis holds the Pritzker Chair at the Center for Strategic and International Studies in Washington DC. Before joining CSIS, he was a diplomat and a member of the US Government's Senior Executive Service. He has extensive negotiating, politico-military, and regulatory experience. He led the first U.S. delegation to the Wassenaar Arrangement Experts Group and developed groundbreaking policies on satellite remote sensing, encryption, high-tech exports to China, and cybersecurity. Lewis was rapporteur for three UN Groups of Governmental Experts on Information Security and his work on norms and confidence-building measures is foundational for international cybersecurity. He has authored numerous publications, is frequently quoted in the media, and has testified numerous times before Congress. His current research looks at cybersecurity, quantum technologies, spectrum-using technologies, and the political and economic effects of the digital revolution. He received his PhD from the University of Chicago.

Cyber Diplomacy: Concepts and Core Competencies

Heli Tiirmaa-Klaar

The rise of cyber diplomacy

With the internet rapidly evolving into an essential environment for human activities, and ICT spreading at an unprecedented pace, laden with software and hardware vulnerabilities, cyber risks are posing an urgent threat that increasingly overshadows the digital transformation. While global connectivity and economic opportunities have flourished, cybercrime has become the most profitable form of organised crime. Military and espionage-related cyber operations have evolved into routine instruments of statecraft, compelling governments to restructure their institutional frameworks. In response, many nations have established specialised national cyber agencies, cyber commands and dedicated cybercrime units. As cyber threats have emerged as a critical concern for national security and foreign policy, a new profession – cyber diplomacy – has taken shape, with cyber diplomats leading international negotiations, preventing conflicts, and fostering agreements in global and regional cyber forums.

The discipline of cyber diplomacy has its roots in the increasingly adversarial state behaviour in cyberspace that became a serious national security concern in the mid-2000s. Although the complete history of cyber conflict is not written

yet, partly due to the opaque nature of the domain and the veil of secrecy governing states' cyber activities, some good analyses on early cyber conflicts exist already.[1]

Intrusions into government classified networks, such as the Moonlight Maze cyber operation against the US, have been taking place since the 1980s. The formative phase culminated with the first large-scale coordinated cyber campaign against Estonia in 2007 and with cyber sabotage to aid the military ground assault during the Russian invasion of Georgia in 2008. This period also saw other notable cyber operations that affected state capabilities, such as the disruption of Iran's nuclear enrichment facility by the Stuxnet computer virus in 2009–2010. After Russia's first incursion into Ukraine in 2014, a new wave of cyber operations had regional and global impact, the most notorious being the NotPetya ransomware in 2017, which affected tens of thousands of targets in Ukraine and other parts of Europe. COVID-19 only accelerated online threats, as did the new Russian invasion of Ukraine in 2022.

With many examples from the growing field of covert cyber operations, including the loss of sensitive government data, rampant cyber espionage, intrusions into critical networks and the continued online theft of intellectual property, the scope of malicious state-organised cyber activity has expanded rapidly.

Cyber diplomacy is a discipline that studies the behaviour of states and other international actors across a wide range of activities manifested in cyberspace. Unlike many other areas of

[1] Healey, J. (2013). A fierce domain: Conflict in cyberspace, 1986 to 2012.

traditional foreign policy, cyber diplomacy addresses not only complex interdependent relationships between governments, but also relationships between governments, the private sector and civil society. Cyber diplomacy requires knowledge in many different fields, including international relations, political science, security studies, economics, digital technologies, cybersecurity, internet governance and development cooperation. A central focus of cyber diplomacy is on international security, as states seek ways to prevent and regulate interstate conflict in cyberspace, build confidence and forge frameworks for cooperation. The political aspects of the multistakeholder internet governance model, protecting human rights online, and the role of new technologies in modern conflicts are also key areas that demand the attention of diplomats.

If traditional diplomacy remains mostly concerned with state-to-state relations in its various formats, in the case of cyber diplomacy the number of stakeholders will be much higher as the private sector, academia and civil society also play important roles in building, innovating and maintaining the functionality of cyberspace. The cyber diplomacy agenda for interstate relations is concerned with bilateral and multilateral cooperation mechanisms to promote international stability, security and cooperation in cyberspace issues, as well as cybersecurity capacity-related assistance. Adjacent issues such as the protection of human rights online, internet governance and technology-related foreign economic policy are also addressed. Governments have begun to broaden their cyber-diplomacy portfolios to include all other foreign policy

implications related to new technologies, such as military use of AI or the role of digital technologies in modern conflicts.

New departments and units dedicated solely to cyber issues have emerged in diplomatic services. As cyber threats grow, a need for international negotiators has emerged, requiring foreign ministries to create the necessary expertise and focal points. The extent to which nations wish to participate in the rapidly evolving field of international cyber affairs will depend on their level of ambition, and whether they choose to establish a large stand-alone structure or devote a small number of foreign service officers to the task. Ideally, a stand-alone cyber diplomacy department or unit should be established to build competence in international cyber and technology issues and provide relevant expertise to regional and functional sections of the foreign service. For nations that are not interested in or cannot afford to create a separate cyber-diplomacy structure, the creation of a taskforce structure with a small number of dedicated diplomats to coordinate international cyber activities with other departments, such as security policy, international organisations, foreign economic policy, human rights, international law and key geographic departments, could be beneficial.

However large or small a dedicated cyber-diplomacy structure is, it should have the right mix of expertise from different fields. In addition to general experience in international security and multilateral negotiations, there is a need for specific expertise in cyber threats, cyber operations, emerging technologies, internet governance, human rights and capacity building. The résumé of a good cyber diplomat would ideally include some

knowledge of national security-related cyber challenges, or prior work experience with similar domestic intelligence and defence counterparts. A minimum number of diplomats to cover all these areas would be five to seven, but a larger team would allow for a more professional approach and competitive edge, as well as better visibility at global cyber fora.

The cyber diplomacy team will also be tasked with mainstreaming cyber issues across the foreign affairs ministry. The lead cyber diplomat, ideally with ambassadorial rank, would benefit from direct access to the foreign ministry leadership and a seniority level that allows for rapid outreach to all heads of overseas missions. Cyber diplomats can educate and raise awareness among their colleagues in the ministry by sending out reports, overviews, lines to take and other useful materials that introduce the topic or provide updates on current cyber issues. Short training sessions for senior political diplomats and ambassadors could be organised on a regular basis. Cyber-diplomatic teams themselves should ensure that all team members receive training on the subject. At present, there are limited opportunities to study cyber diplomacy as a separate subject, but there are some academic courses on various topics related to cyber diplomacy. International conferences and workshops are also a good training ground for those new to the field.

Threats in cyberspace

In the context of imperfect information technology ecosystems and an increasing number of cyber threats, policymakers may find it useful to conceptualise cyber risk according to the level of impact of these threats. By analysing cyber vulnerabilities at the global, national, sectoral and individual levels, policymakers can identify solutions to adequately assess and respond to the cyber risks they face.

At the *global level*, technological or man-made disruptions to IT systems could result in large-scale economic loss or disruption. In 2017, a globally spreading ransomware campaign, NotPetya, attributed to Russian intelligence services, affected not only its original targets in Ukraine, but also many Western companies, with an estimated cumulative cost of $10 billion, as the ransomware virus caused serious disruptions in many economic sectors worldwide. The global impact of cybercrime multiplied during the COVID-19 pandemic, and ransomware continues to plague digitalised economies.

Diplomats and national security experts are mostly concerned with cyber threats that affect *nation states*. Cyber operations against nation states are organised by states or state-sponsored actors, and are conducted either in peacetime, or in wartime in support of conventional military activities. State-organised cyber operations can also support hybrid conflicts or constitute stand-alone activities aimed at obtaining data for espionage, discrediting a country's national security interests, or interfering in elections or other internal political and social processes of a foreign country.

Many cyber threats can cause disruption or malfunction of one or more critical *economic sectors or industries*. The growth of ransomware attacks has affected many industries and critical sectors. Economic espionage in cyberspace against a company or group of companies can cause significant economic loss or create market distortions and disadvantages. Further advances in technology, such as AI, will multiply cybercrime techniques.

Finally, many cyber threats can have an impact at the *individual end-user level*, either affecting a private computer user or as an aggregated effect of hostile influence. For example, home users' PCs with weak cybersecurity protection could be hijacked and added to the 'botnet armies' used for illegal activities online. Individuals using the internet could also become the weakest link in digital value chains, because of either human negligence or a lack of awareness of privacy and personal data protection when conducting online activities.

Cyber diplomacy is mostly concerned with finding policy solutions to address cyber threats on the global and nation-state levels, whereas national cyber agencies will concentrate on policy responses to fight cyber threats affecting different economic sectors and end-users.

Definition of cyberspace

A comprehensive description of cyberspace is provided by the US National Institute of Standards and Technology (NIST). According to NIST, cyberspace is 'the interdependent network of information technology infrastructures, and includes the

Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries'.[2] This description implies that cyberspace captures a wider digital ecosystem, which can be but is not necessarily connected to the internet. The internet provides a platform for connectivity for all the different open digital systems, making it an interdependent network of networks. However, there are also elements of cyberspace that are not connected to the Internet, such as industrial control systems of critical infrastructures that provide us with essential services such as electricity, water and transport. Closed information systems are separated from the world wide web, including specific military, intelligence, industrial and other communications systems with restricted access.

Cyberspace is made up of many technological elements woven together by the ICT and telecommunications backbone infrastructure and using the logical and physical internet infrastructure. Unlike the other domains—air, space, land and sea—cyberspace is a man-made construct. Software and hardware in the cyber domain have historically been created by programmers, engineers, computer scientists and other experts, although the recent trend is for software to be increasingly created by AI tools. The information technology architecture of a large organisation typically includes thousands of ICT components produced by different companies, with individual components often produced by

[2] CSRC Content Editor. (n.d.). *cyberspace - Glossary | CSRC*. https://csrc.nist.rip/glossary/term/cyberspace

different IT development teams. The cumulative complexity of such systems can be enormous. Given that most organisations have built their IT systems over the past 30 years or more, the layers of technology generations and products add to this picture. Because of the complexity of the whole domain, there are many vulnerabilities that can be exploited, ranging from software bugs and other technological weaknesses to traditional human negligence that allows attackers to penetrate IT systems. With sufficient resources and determination, most IT systems can be accessed by third parties. According to IBM, the average time to discover a data breach in an organisation's IT systems is 197 days, and the average cost of a cyber incident for an organisation was $4.8 million in 2024.[3]

Core competencies of cyber diplomats

Like many other diplomats, cyber diplomats should cover a wide range of interrelated issues and be able to move quickly between complex subject areas. For example, decision-making on international security issues may be informed by the latest developments on internet governance, or a request for cybersecurity development cooperation may be rejected because of a country's questionable online rights practices. In addition, any cyber diplomacy unit should have a diverse set of skills, ranging from a good understanding of cyber technologies to solid negotiation experience: qualities that are

[3] *Cost of a data breach 2024 | IBM*. (2024). https://www.ibm.com/reports/data-breach

not often found in one person. Diplomats who have been assigned cyber portfolios find themselves in a difficult position, wondering what they should study to become proficient in the field. The following section lists the core competencies that cyber diplomats should acquire, either individually or as dedicated teams in diplomatic services.

International security and responsible state behaviour in cyberspace

Matters of war and peace have been at the core of diplomacy since ancient times. The first and probably greatest challenge for cyber diplomats is to learn what formal and informal rules, norms and principles govern state behaviour in this domain in the context of international security. The framework of responsible state behaviour consists of the application of existing international law governing state activities in cyberspace, the implementation of norms of responsible state behaviour, confidence-building measures, and capacity building in cyberspace. Each of these four elements includes several activities in global and regional organisations or other multilateral formats that cyber diplomats should follow on a regular basis.

The complexity of ICT systems makes it almost impossible to build a classical arms control regime in cyberspace. With dual-use IT technologies, it is not possible to verify that signatories to an international cyber arms treaty are complying with their legal obligations, as is the case with nuclear, biological and

chemical weapons. Moreover, it is difficult to define what a cyber weapon is, let alone verify its use, so the only realistic approach currently is to rely on regulating state behaviour. Similarly to climate agreements, regulating state behaviour means that governments honour their commitments and behave responsibly by following the rules of the road in cyberspace. These rules were negotiated and agreed by the UN General Assembly, based on the recommendations of the reports of the UN Group of Governmental Experts on cybersecurity in 2009–2021.[4]

A foundational knowledge for cyber diplomats is the understanding how *international law* applies to states' cyber activities. At the UN level, there is a consensus that both international humanitarian law (IHL) and customary international law apply in cyberspace, which should cover all activities of states below and above the threshold of international armed conflict. It is well understood that IHL covers state behaviour when cyber operations produce kinetic effects equivalent to an armed attack. When planning cyber operations in time of war, states should follow the IHL principles of necessity, proportionality, distinction and humanity, the same principles they are obliged to follow on land, sea, air and space. It is also agreed that the UN Charter applies in the cyber context, meaning that states have the 'right of individual and collective self-defence in the event of an

[4] All UN GGE reports are accessible at UN Office of Disarmament website: UN Office of Disarmament. (n.d.). *Developments in the field of information and telecommunications in the context of international security*. https://disarmament.unoda.org/ict-security/

armed attack against a Member of the United Nations'. A number of states have articulated what they consider to be the threshold of an armed attack in the cyber domain, such as cyber operations that result in a level of death and destruction equivalent to that of an armed attack, and may trigger a state's right of self-defence under Article 51 of the UN Charter.

The well-established rules of customary international law also guide state behaviour. Unlike the body of law that applies above the threshold of an armed attack, customary law consists of state practice and *opinio juris*, evidence of a state's understanding of its legal obligations. The sources of customary law may be treaties, decisions of national or international courts or other examples of state practice. For example, the law of state responsibility addresses important issues such as what constitutes a breach of international obligations, the definition of internationally wrongful acts, and the legal clarity of attribution and the adoption of countermeasures. While most states agree that states should be guided by the principles of customary law, they may interpret the nuances of how state practice shapes state behaviour. As the practice of states in conducting cyber activities is still evolving and views are still forming, a useful source for the applicability of international customary law is the 'Official compendium of voluntary national contributions on how international law applies to the use of information and communication technologies by States, submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to UN General Assembly

resolution 73/266 (A/76/136)', annexed to the 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135)'.[5]

The next critical building block in the framework of responsible state behaviour is *voluntary peacetime norms*. Described in the abovementioned consensus reports, the development of these norms has been a long and painstaking process in the UN First Committee over nearly two decades, codifying the main principles of state cyber behaviour in peacetime. These 11 norms could be analysed in different categories, such as whether they are prohibitive or permissive, whether they reflect principles already established by existing international law, or whether they are cyber-specific. It does not matter whether the norms are general rules for state behaviour or are derived from the cyber context. What matters is that they provide general guidelines for appropriate international cyber behaviour for states. And interestingly, with few exceptions, the majority of UN member states follow these norms in their daily cyber activities. The violation of norms by reckless states does not mean that norms do not provide useful guidance for the large number of countries that want to be good cyber citizens. Norms encourage cooperation, assistance, the protection of critical information infrastructure, the sharing of information

[5] United Nations. (2021). Report of the Group of Governmental Experts on Advancing Responsible state Behaviour in Cyberspace in the context of International security. In *United Nations* (pp. 1–26) [Report]. https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf

and responsible reporting of vulnerabilities, and the protection of human rights and privacy online. Norms also prohibit certain types of activity, such as internationally wrongful acts emanating from a country's territory or supporting activities that violate international legal obligations. An important cyber-specific norm is that Computer Emergency Response Teams (CERTs) should not be harmed or used to harm similar teams. This norm is central to contributing to the stability of cyberspace, as CERTs are tasked with keeping the global internet up and running by mitigating cyber threats on a 24/7 basis.

Cybersecurity confidence-building measures (CBMs), derived from the Cold War stabilisation mechanisms, have proved to be essential cornerstones of regional cyber cooperation. The OSCE, the ASEAN Regional Forum and the OAS have used these measures to promote cybersecurity cooperation, increase transparency and create peer-learning networks at the regional level. Regional organisations often act as catalysts for the exchange of best practices and transfer of knowledge among regional partners. CBMs also promote transparency and stability. For example, the OSCE's Points of Contact (POCs) provide an operational capability to alert partners in the event of a major cyber incident and provide for regular communications checks, which acts as an effective early warning mechanism. Confidence-building activities also include consultation and cooperation, the exchange of information on threats and vulnerabilities, the exchange of national strategies and policies, the protection of critical infrastructure, and the promotion of capacity-building and public–private partnerships.

There is a broad consensus among UN member states that *cyber capacity building* is a key component of a framework for responsible state behaviour in cyberspace. UN member states have very different levels of technological capacity, cyber preparedness and institutionalisation of cyber organisations. There are several indexes and cyber maturity models that assess nations' cyber readiness and identify gaps. Many useful cyber capacity-building programmes and projects have been implemented by governments and international organisations that focus on cyber capacity of transition and developing countries. The Global Forum of Cyber Expertise seeks to provide an overview of all bilateral and multilateral capacity-building programmes and acts as a global umbrella organisation for the cyber capacity-building community, where best practices and other relevant knowledge can be shared. The World Bank has established a Cybersecurity Multidonor Trust Fund for capacity building, and the EU, US and other governments have specific programmes with annual earmarked budgets. Cybersecurity capacity building remains largely a niche issue for the large development assistance community, which often views cybersecurity as a national security issue. However, with digital trust and cybersecurity being an integral part of any successful digitalisation project, a paradigm shift is long overdue in the development community to see cyber insecurity as a serious impediment to the economic and social progress of developing countries. Funding for cyber capacity building should increase, and the OECD Development Assistance Committee could open a separate funding line in its Official Development Assistance (ODA) workbooks. Mainstreaming cyber capacity building into ODA would help Western nations to allocate more meaningful

funding to cyber projects in technologically less developed countries.

Internet governance

As the Internet has evolved from an academic project to a global platform vital for all social and economic activities, its governance model has retained its original features, whereby all key stakeholders—civil society, the private sector and governments—play an equal role. Internet governance refers to the processes, policies and mechanisms that influence the management and development of the global internet. It encompasses the technical infrastructure, legal frameworks and norms that govern the way the Internet operates. A critical aspect of Internet governance is its multistakeholder model, which brings together diverse groups including governments, the private sector, civil society, technical experts and international organisations. This model ensures that no single entity has control over the Internet and promotes an inclusive approach whereby different perspectives contribute to decision-making. The multistakeholder model has been instrumental in creating a decentralised and global internet that can promote innovation, freedom of expression and access to information.

Cyber diplomats will need, at minimum, an understanding of a large internet governance ecosystem of different bodies, cooperation mechanisms and international processes that develop, coordinate, and regulate the internet resources. The Internet Corporation for Assigned Names and Numbers

(ICANN) plays a critical role in this landscape by managing the global Domain Name System (DNS), ensuring the uniqueness and accessibility of web addresses, and overseeing the allocation of domain names and IP addresses. ICANN operates on a multistakeholder model, involving governments, the private sector, technical experts and civil society in its decision-making to ensure the stable and secure operation of the internet.

The Internet Governance Forum (IGF) is a global multistakeholder platform established by the United Nations to discuss public policy issues related to internet governance. It brings together representatives from different sectors to exchange ideas and best practices, although it has no formal decision-making powers. The World Summit on the Information Society (WSIS), another UN-sponsored initiative, focuses on bridging the global digital divide and promoting an inclusive information society. The WSIS has contributed to the establishment of the IGF and has identified lines of action to guide global efforts in areas such as internet access. Regional Internet Registries (RIRs) manage the allocation and registration of IP addresses within specific regions and ensure the efficient distribution of IP addresses globally through coordination in the Number Resource Organization (NRO). Finally, the World Wide Web Consortium (W3C) develops open standards that ensure the long-term growth of the web, enabling seamless operation and universal accessibility regardless of users' hardware, software or physical limitations.

The private sector and civil society have an essential role to play in shaping a free and interoperable internet. Companies that

provide internet infrastructure and services contribute technical expertise, drive innovation, and set industry standards that ensure interoperability and accessibility. Meanwhile, civil society organisations attempt to protect human rights online, such as privacy, freedom of expression and digital inclusion. Together, these stakeholders balance commercial interests with the public good, helping to maintain an open internet that is resilient to censorship and manipulation, while supporting economic growth and social development on a global scale.

Internet freedom and human rights online

These revolve around key principles that ensure the internet remains a space for open communication, free expression and equal access to information. At its core is the right to freedom of expression, which allows individuals to share ideas and access information without undue censorship. Privacy and data protection are equally crucial, protecting individuals' personal information and ensuring control over how their data is used. A growing number of national and regional regulations are shaping privacy and data protection regimes around the world.

Access to information is another fundamental aspect, emphasising that the internet should be open and accessible to all, allowing people to seek and share content freely. This is closely linked to the right of assembly and association online, whereby individuals can form communities, engage in collective action and participate in online discourse without fear of repression. Digital inclusion is essential to bridging the digital divide by ensuring that everyone, regardless of their

background, has access to the internet and the tools to use it effectively. Accountability and transparency are important to hold governments and companies accountable for their actions that affect internet freedom, and to ensure that decisions about governance, content moderation and data practices are made openly and fairly.

Several forums and organisations work to protect these principles. The Freedom Online Coalition is a prominent group of countries committed to advancing internet freedom and protecting human rights online. The Electronic Frontier Foundation advocates for digital rights, focusing on issues such as privacy, free expression and innovation. Access Now is another key organisation that defends digital rights, particularly focusing on ensuring an open and secure internet. These and many other forums play a critical role in promoting and protecting human rights in the digital sphere.

Cyber operations

Cyber diplomats should understand the basic elements of computer network operations to assess conflicts in cyberspace or respond to malicious cyber activities. In order to exploit the adversary's networks, the technical methods of penetrating information systems are quite similar in any cyber operation, whether for warfare or espionage. The line between cyber espionage and warfare is thin and is also the reason why cyber operations are more difficult to understand, label and attribute than traditional espionage or military operations.

Computer network operations include:

1. *Computer network attacks* involve actions taken to disrupt, deny, degrade or destroy information stored on computers and computer networks, or the computers and networks themselves. These actions may be conducted by electronic means or by other means, such as physical destruction or deception.
2. *Computer network defence* refers to actions taken to protect, monitor, analyse, detect and respond to unauthorised activity within information systems and computer networks.
3. *Computer network exploitation* includes actions taken to infiltrate, collect, extract or manipulate data or information contained in computers and computer networks for intelligence or other purposes.

The cyber operation or intrusion begins with reconnaissance, where attackers research potential targets and identify vulnerabilities, connected third parties and existing or new entry points. This phase sets the stage for weaponisation, where attackers develop or modify malware based on the information gathered during reconnaissance.

This is followed by the delivery phase, where the malware is sent to the target, often through phishing emails or by exploiting network vulnerabilities. Then comes the exploitation, where attackers use discovered vulnerabilities to infiltrate further, often moving laterally across the network. The final steps include the installation of malware to take control of the system, and command and control, where attackers

communicate with the installed malware to carry out their objectives, such as data exfiltration or network disruption.

Attribution

The importance of cyber detection and attribution cannot be overstated, particularly in the context of state actors' accountability. As cyber threats continue to evolve and become more sophisticated, accurately identifying the perpetrators of malicious cyber activity is critical to holding state actors accountable for their actions in cyberspace. Cyber-detection capabilities allow for the timely identification of cyber intrusions and enable rapid response to mitigate their impact.

Fortunately, the attribution techniques have evolved over time, and it has been easier to identify the individuals, groups or nation states responsible for cyber incidents. Attribution also serves as an important element in preventing future malicious behaviour. By accurately attributing cyber operations to specific state actors, the governments can impose diplomatic, economic or legal consequences, thereby fostering a more accountable and secure cyberspace. In addition, attribution could possibly serve as a long-term deterrent, sending a clear message to state actors engaging in malicious cyber activity that it will not go unnoticed.

Cyber warfare

Cyber warfare has emerged as a distinct domain of operations in which nations pursue strategic objectives by exploiting and defending against cyber vulnerabilities. In this domain, objectives often include disrupting enemy infrastructure, gathering intelligence, undermining command and control systems, and protecting critical national assets from cyber threats. Countries are investing heavily in developing specialised cyber capabilities and forming dedicated cyber forces to effectively support and execute these objectives.

While the global community of cyber policymakers and practitioners is still searching for an appropriate analytical framework to approach the strategic and operational dimensions of cyber conflict, we have a relative lack of doctrinal clarity for conducting cyber operations in wartime.

To draw a parallel with nuclear conflict strategies: it took decades of effort to develop doctrines and conflict prevention mechanisms after the first use of nuclear weapons. A nascent cyber-diplomatic community has begun to develop the appropriate frameworks for conflict prevention and stability in cyberspace, including the above-described framework for responsible state behaviour. Encouragingly, democratic cyber powers have integrated respect for international law and the promotion of cyber norms into their respective military cyber strategies, contributing to overall stability and predictability of state behaviour in cyberspace.

Cyber espionage

Cyber espionage and traditional espionage share many similarities because the goal remains the same: to gather political, commercial or military information. Cyber espionage exploits the anonymity, global reach and asymmetric nature of the internet. The interconnectedness of information networks and opportunities for deception provide plausible deniability, although attribution methods have evolved rapidly, and deniability has become more complex.

The most common targets of cyber espionage are large corporations, government agencies, academic institutions, think tanks or other organisations that possess valuable intellectual property and technical data that can provide a competitive advantage to another organisation or government. Targeted campaigns may also be conducted against individuals, such as prominent political leaders and government officials, business executives and even celebrities.

Economic and industrial espionage, including cyber espionage, poses a significant threat to a nation's prosperity, security and competitive advantage. Cyberspace is a preferred operational domain for many threat actors, including nation states, state-sponsored groups, organised crime and individuals.

Cyber economic espionage targets organisations to gain access to and steal trade secrets and intellectual property. It can require a high level of technical sophistication and lengthy preparation to evade common malware detection methods.

Cybercrime

While it is possible that future technological advances will result in more secure software and hardware products with built-in security by design, most organisations are currently operating with a vulnerable technological base. As discussed above, due to complexity and many other reasons, current IT systems are still vulnerable and provide opportunities for hackers and criminal groups to exploit the weaknesses in cyberspace. With 5.5 billion internet users worldwide in 2024 and 30.9 billion connected devices expected by 2025, economies and societies are more dependent than ever on ICT.[6] The widespread use of AI and the growing number of Internet of Things (IoT) devices are accelerating new cyber vulnerabilities. Against this backdrop, cybercrime has flourished and is seriously affecting all economies and societies. Ransomware remains a dominant threat, with 2024 potentially setting a record for ransom payments.[7] Attackers are using AI to improve their tactics, making malware more effective and social engineering attacks harder to detect. Several estimates predict that cybercrime losses will reach astronomical levels in coming years due to AI-powered intrusion methods.

---

[6] Statista. (2024, December 12). *Global number of internet users 2005-2024*. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

[7] Page, C. (2024, October 31). 2024 looks set to be another record-breaking year for ransomware — and it's likely going to get worse. *TechCrunch*. https://techcrunch.com/2024/10/31/2024-looks-set-to-be-another-record-breaking-year-for-ransomware-and-its-likely-going-to-get-worse/

Diplomats are involved in several international negotiations to combat cybercrime, such as promoting the Council of Europe Convention on Cybercrime and following a UN Convention on Cybercrime adoption. They also help developing countries develop legal frameworks for prosecuting and investigating cybercrime, build cybercrime capacity in law enforcement, and facilitate training and education for national judicial structures in partner countries.

A short history of international cyber cooperation

As a result of the 2007 cyberattacks, the Estonian government began to promote cybersecurity on the agendas of major international organisations, such as NATO, the EU, the OSCE and the UN. The first organisation to provide a policy response to cyber threats was NATO, which included cyber defence in its policy agenda and issued the first NATO Cyber Defence Policy in 2008. NATO's 2009 Strategic Concept notes that 'adversaries, both state and non-state, may seek to exploit the Alliance's increasing reliance on information systems through information operations designed to disrupt such systems. They may seek to use such strategies to counter NATO's superiority in traditional weapons.[8]

[8] NATO. (2012, July 30). *Towards the new strategic concept - A selection of background documents*. https://www.nato.int/cps/en/natohq/topics_82717.htm

NATO is also the first international organisation to establish an internal cyber-defence governance structure that protects its entire command structure and headquarters on different continents. In 2011, a separate new Cyber Defence Committee was added to NATO's consensus-based policy-making structure, advising the North Atlantic Council at the International Staff at NATO Headquarters on cyber matters. An important milestone in the development of NATO's cyber policy was the decision in 2016 to declare cyberspace an operational domain. This has accelerated the process of incorporating cyber elements into defence planning and military operations in all NATO members, as well as the establishment of dedicated cyber forces within Allies' national military structures.

In 2021, NATO's most recent cyber defence policy promised to use the full range of capabilities to actively deter and defend against the cyber threats, including by considering collective responses. Responses will draw on elements from the entire NATO toolbox, including political, diplomatic and military instruments. The policy also sets out that the effects of significant malicious cumulative cyber activity could, in certain circumstances, be considered an armed attack, which could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty.[9]

As an important building block of existing international cyber-diplomacy frameworks, regional organisations have played a

[9] NATO. (2021). *NATO Cyber Defence*. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf

central role in establishing cybersecurity policy discussions and cooperation mechanisms. The first regional cybersecurity discussion was organised by the Estonian government at the OSCE in March 2008. The event brought together diplomats, military commanders, heads of national cyber agencies and academic experts. Cyber discussions continued in the OSCE, culminating in the establishment of an Intergovernmental Working Group on Cyber Issues, which continues to this day and has served as an instrumental body for the development and implementation of regional CBMs over the past decade. Cyber CBMs contribute to overall security and stability in the OSCE region by promoting responsible state behaviour and fostering cooperation in the field of cybersecurity. OSCE cybersecurity CBMs aim to enhance trust, reduce tensions and build confidence and capacity among states, as well as to facilitate dialogue and cooperation to address cyber threats.

The OSCE cybersecurity CBMs include the establishment of a network of contact points, early warning and information sharing mechanisms, exchange of national strategies and doctrines, and holding joint thematic workshops. The two sets of OSCE regional CBMs adopted in 2013 and 2016 have also set an example for other regions that have followed suit and established regional cybersecurity confidence building mechanisms in the ASEAN Regional Forum (ARF), the OAS and others.

Two regional organisations stand out as exemplary facilitators of regional cyber cooperation and peer learning in cyber resilience building. First, the *OAS* has been active in the field of cybersecurity for a decade, organising training, workshops and

exercises for various cyber actors in Latin American states. Despite having a small staff and limited resources, the OAS has been a visible actor on the global cyber scene and its programmes have benefited many countries in the region. The OAS has also been active in helping its member states develop cyber resilience programmes and promote confidence and capacity building at the regional level. The OAS Inter-American Cooperation Portal on Cybercrime and its Cyber Security Programme are among many examples of useful regional efforts in Latin America.

Similarly, *ASEAN* has emerged as a good example of regional cooperation, with more advanced member states taking the lead in establishing the normative framework of voluntary cyber norms and ensuring their adoption by all regional governments. ASEAN ministerial meetings have addressed cyber issues on several occasions, and Singapore has created an ASEAN Singapore Cybersecurity Centre. The ASEAN Regional Forum has discussed measures to promote cyber stability and confidence among its members.

The *African Union* Convention on Cyber Security and Personal Data Protection provides a framework for cooperation among African countries on cybersecurity, data protection, cyber strategy, awareness and capacity building, and information sharing. The African Union has also established a Cyber Security Expert Group to address cyberattacks and cybercrime and to promote cyber cooperation, which must be an integral part of the digital revolution.

As a supranational and international organisation, the *European Union* started to develop its cyber-policy posture later than the

traditional security organisations, NATO and the OSCE. Despite its late start, the EU now has the most extensive cybersecurity cooperation at the regional level, as this organisation enacts 80% of the economic, financial and sectoral regulations for all EU member states. Since the adoption of its first Cyber Security Strategy in 2013, the EU has built up an impressive track record of cyber regulations and policies. Most existing EU cyber policies and legislative initiatives aim to increase overall cyber resilience and strengthen the Union's cyber ecosystem by fostering cooperation, improving technological capabilities and creating a higher level of cyber preparedness in EU member states under its internal market and home affairs competences.

EU cyber policy has evolved rapidly and is characterised by many legislative and non-legislative initiatives. Due to different decision-making procedures in its three areas of competence—justice and home affairs, the internal market and common foreign and security policy—the EU has moved at different speeds on cyber issues in these areas. The EU's most developed cyber-policy area is in the field of justice and home affairs, which has produced a number of legislative changes to combat cybercrime, resulting in all 27 EU countries harmonising penalties, streamlining investigations and promoting cooperation between national police forces in the fight against cybercrime. A number of EU mechanisms include legislation to promote the fight against cybercrime, law enforcement cooperation and the collection of electronic evidence. Several EU agencies and cooperation working groups are involved in the day-to-day implementation of all these many initiatives. The EU has also set up a dedicated agency to deal with the

threat of cybercrime, the European Cybercrime Centre (ECC), which is based next to Europol.

The EU has devoted significant attention and resources to strengthening cyber resilience in its internal market policy area. The two editions of the Network and Information Systems Security (NIS) Directives aim to set higher cyber standards for key economic sectors and public administrations across the Union. The EU Cyber Certification Framework and the Cyber Resilience Act aim to provide more trustworthy technology, while the Cyber Competence Centres network aims to channel additional resources into cyber innovation and research in all EU member states. The 2016 NIS Directive created a standard for all member states to have minimum cybersecurity requirements for critical networks, and to improve cyber-incident response and information sharing. With the Cybersecurity Act 2017, the EU has tasked its cyber agency, ENISA, to work on an ambitious cybersecurity certification scheme that will start assessing ICT products with a single cyber certification to replace fragmented national systems.[10] As the EU also regulates the national policies of its member states in the abovementioned areas, these could be described as supporting cooperation between European countries in important cybersecurity areas, contributing to cyber diplomacy but going beyond traditional foreign policy.

The EU's Common Foreign and Security Policy addresses all matters of foreign policy, diplomacy and security policy. This

[10] European Commission. (2024, November 21). *Cybersecurity*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity

field remains intergovernmental within the EU, meaning that the EU relies in foreign policy issues on the leadership of the member states and their diplomatic services. Since 2017, the EU has adopted several common strategies to respond to malicious cyber activities. Most important among these was setting up a framework that allows member states to provide diplomatic response to cyber activities. The 2017 Council Conclusions 'Framework on a Joint Diplomatic Response to Malicious Cyber Activities' (Cyber Diplomacy Toolbox)[11] has created the first multinational policy framework to find a suitable response to serious cyber activities that fall short of armed conflict but inflict serious damage to economy and society to go unnoticed and unpunished. As a follow-up initiative to this policy measure, the EU adopted a specific regime for applying cyber sanctions in 2019.

A joint framework for responding to malicious cyber activities has been used for coordinated response on state-sponsored cyber operations. The EU has imposed horizontal sanctions on entities and individuals organising cyber operations against EU interests and issued several joint statements attributing and condemning cyberattacks. A nascent EU Intelligence and Situation Centre under the European External Action Service is coordinating information sharing among European countries to provide analysis and syndicated intelligence to support joint decision-making on cyber attribution and the application of sanctions.

[11] EEAS. (2023, February 23). *Cybersecurity*. https://www.eeas.europa.eu/eeas/cybersecurity_en

The *Council of Europe* adopted the Convention for Cybercrime in the early years of advancing global connectivity in 2001. Also known as the Budapest Convention, it provides a common framework for international cooperation for its members and aims to harmonise cybercrime legislation. With its global reach, the Budapest Convention not only offers the most comprehensive guideline for investigating and prosecuting cybercrime but also provides a 24/7 law enforcement network to facilitate information sharing and operational cooperation between its members.

In addition to regional and national efforts, the *United Nations* has been in the centre of cyber-diplomacy efforts with its Group of Governmental Experts on cybersecurity under the Disarmament Committee. Since 2009, this group has developed a normative framework that provides guidance for state behaviour in cyberspace. It consists of existing international law, norms of voluntary peacetime state behaviour, cybersecurity CBMs and capacity building. The group presented its consensus reports to the UN General Assembly (UNGA) in 2010, 2013, 2015 and 2021, adopting a view that international law, the norms of state behaviour and CBMs together with capacity building form a framework for cyber stability and conflict prevention. Currently, the Open-Ended Working Group under the UN Disarmament Committee serves as a mechanism for all UN nations, widening the understanding on norms of responsible state behaviour, CBMs and international law applying in cyberspace. The new UN Programme of Action on cybersecurity that will be established concentrates its efforts on implementing the normative framework and capacity building, which remains a primary interest for many UN member states.

Under the auspices of the UN Third Committee, the UN member states reached agreement on a 'UN convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes' in 2024.[12] Negotiations on the first legally binding UN treaty on cybercrime have been conducted in a tense atmosphere, trying to strike a balance between human rights safeguards and cybercrime concerns.

The role of cyber diplomats in national cyber policy coordination

In addition to international outreach, cyber diplomats should regularly coordinate various international issues with domestic counterparts in the line ministries and agencies. A mature national cyber ecosystem would consist of many different counterparts in specific cyber fields, most of them also having relations with similar agencies in other countries. Therefore, the first task for new cyber diplomats is to attain and maintain an overview as to what kind of international relations the domestic agencies have, whether these relations are in line with the

[12] *Reconvened concluding session of the Ad Hoc Committee*. (n.d.). United Nations: Office on Drugs and Crime. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_reconvened_concluding_session/main

country's larger foreign policy goals, and whether there are gaps that should be filled in terms of international outreach. Ideally, national cyber policy should be coordinated by some governmental entity where the Ministry of Foreign Affairs (MFA) should also be invited to take part. In cases where the MFA has been part of national cyber coordination since its formation, those relationships will have evolved over time naturally and there will already be an overview on the division of labour. For diplomats that are new to cyber issues and MFAs that are just starting to build their cyber diplomacy expertise, reaching out to national counterparts should be a priority. Although there are many global, regional and other international priorities, all cyber diplomats should be able to represent their national whole-of-government approach on cyber issues internationally. In addition, it will usually help the coordination efforts if the MFA creates an inter-agency working group for coordination on international cyber cooperation issues.

There are specific cyber-policy communities in each country that shape national efforts. First, and most importantly, there should be an agency responsible for coordinating cyber-resilience issues and overseeing critical information infrastructure protection (CIIP). This agency will issue and oversee cybersecurity regulations for essential service providers and government agencies. In some larger countries, the role of CIIP is shared between the national cyber agency and sectoral regulators in critical sectors such as energy, transport and finance. This agency should also liaise with the private sector and conduct regular national cyber exercises and cyber-threat awareness campaigns. In EU legislation, these agencies are called National Competent Cyber Authorities. As a testament to

the novelty of the whole cyber issue, these authorities are part of very different chains of command in different nations. In some countries, they are part of the communications, transport or interior ministries; in others, they are part of the prime minister's office; in others still, they are part of the defence or intelligence services. The national cyber architecture depends on the specific national institutional set-up, and each nation has chosen its own way of organising its cyber structures. Many national cyber agencies have active relationships with their counterparts in other nations, and diplomats should be aware of these relationships and, where appropriate, help to establish them.

In the context of cyber-resilience efforts, a very important national counterpart is the technical community for mitigating cyber incidents, i.e. CERTs, which are technical units tasked with mitigating cyber problems on a 24/7 basis. Depending on the size of the country, there may be many CERTs at federal, regional or sectoral level. Most countries have a government CERT and a national CERT that acts as a national POC for similar entities in other countries. The closest analogy to CERTs in the physical world would be fire brigades: CERTs actively address cyber problems in real time on specific networks. They prevent, respond to, mitigate and help recover from cyber incidents, and also coordinate information sharing, identify cyber vulnerabilities, provide early warning and ensure technical response to cyber incidents. CERTs also work closely with their foreign counterparts, as data moves across borders at the speed of light. As the CERT community has existed since the first serious cyber incidents in the 1990s, they have been the guardians of the vast cyber galaxy before many other national

or international cooperation mechanisms were set up. CERTs have their own international organisation, FIRST, which ensures coordination between them and, very importantly, vets the various CERT entities, public or private, as legitimate 'cyber fire brigades', because, as discussed above, cyberspace is a complex dual-use domain and a generalist without prior professional knowledge would not be able to distinguish between legitimate and illegitimate actors without prior authentication. Therefore, professional vetting should take place to ensure that all FIRST members are in the camp of 'guardians of cyberspace'.

The second important group of national stakeholders is the national law enforcement agencies that oversee the investigation and prosecution of cybercrime. In each country, there is a dedicated cybercrime structure within the criminal police organisation, as well as judges and prosecutors who deal with cybercrime matters. A key component for the criminal justice community would be to have a national legal framework to deal with cybercrime. In this regard, the Budapest Convention has served as a blueprint for many nations on how to establish national legislation and cross-border cooperation to combat cybercrime.

The third community with which cyber diplomats should develop close ties is the national intelligence community. The intelligence community would be knowledgeable regarding sophisticated cyber threats and have insight into advanced persistent threat (APT) actors targeting countries' government and private sector networks. Building strong relationships with the intelligence community would also be critical to

establishing a national coordination mechanism for attribution of cyberattacks. To date, many countries have already developed national attribution guidelines and related attribution coordination involving a variety of national stakeholders, with the intelligence community as a central partner organisation in these efforts.

The fourth group of national stakeholders with which cyber diplomats should coordinate their efforts are cyber-defence and military structures. Critical military networks are usually independently operated and regulated by defence command chains, monitored by specialised military CERTs. In many countries, cyber commands have been established to implement the tasks of cyber protection of military assets and the development of military cyber capabilities. National Cyber Commands are tasked with performing national cyber defence functions in wartime. Preparing for wartime cyber activities means that they are closely involved in peacetime national cyber coordination. Many Cyber Commands also have close relationships with their partner organisations in allied countries and participate in the various international military-to-military cooperation formats and exercises, such as NATO Cyber Coalition exercise.

Traditionally, all of the national actors described above have operated under the authority of different ministries, departments and political overseers. Recently, however, there has been a trend to unify national operational technical civilian, military and intelligence capabilities under one umbrella structure to streamline the response to cyber threats along the criminal, defence and intelligence axes.

Future challenges for cyber diplomats

Cyberspace remains an asymmetric domain, where the private sector defines its contours and state policy responses often lag. The rapid evolution of digital technology is profoundly reshaping the dynamics of current and future conflicts and, by extension, interstate relations. To navigate this landscape, the role of diplomats becomes both crucial and challenging. Diplomats must increase their expertise and expand their ranks. Stabilising this volatile domain requires a deep understanding of international law, CBMs and normative frameworks. Currently, cyber commands and forces employ many orders of magnitude more personnel than cyber-diplomatic teams, which can still fit into one large conference room at the United Nations. As advances in AI and quantum computing redefine cyber-threat vectors, collaboration with the private sector and academia is essential to understand and mitigate emerging threats. Leveraging the technical expertise of national cyber agencies and ensuring robust training opportunities for future diplomats will further strengthen these efforts.

There are several areas that diplomats should focus on to advance this emerging area of foreign policy. First, advancing accountability and enforcement of existing agreements on responsible state behaviour in cyberspace should remain a priority. As attribution techniques improve to better identify perpetrators, states must act more decisively upon such revelations. While sanctions for malicious cyber activity have shown some effectiveness, there is still room for likeminded nations to refine their policy responses, including by using

powerful economic and trade tools to influence aggressive cyber actors.

Second, further improving cyber resilience and capabilities is imperative. Disparities in cyber preparedness and technological sophistication among nations hinder the implementation of frameworks for responsible state behaviour in cyberspace. Leading cyber nations and democratic powers should actively assist intermediate and less technologically advanced countries in developing expertise and establishing robust legal and institutional frameworks to counter cyber threats. Intensifying global efforts to assist nations in need of external support will further stabilise the international cyber landscape.

Finally, to counter future technology-enabled threats and stabilise the cyber domain, likeminded democratic nations must cultivate not only technical capabilities but also thought leadership on strategic technological stability. This includes deepening expertise on the impact of new technologies on modern conflict, clarifying the application of international law and norms in cyberspace, and fostering collective insights to ensure long-term stability. Given the accelerated pace of digital innovation compared to the early nuclear era, there is an urgent need to formulate more robust policy responses to the impact of new technologies on strategic stability. Addressing the technological aspects of modern conflict requires foresight, interdisciplinary collaboration and proactive policy development, in which diplomats should play a central role.

Heli Tiirmaa-Klaar

Visiting Distinguished Fellow at the German Marshall Fund (GMF) and chairs the IT Coalition assisting Ukraine

Heli Tiirmaa-Klaar is a Visiting Distinguished Fellow at the German Marshall Fund (GMF) and chairs the IT Coalition assisting Ukraine. Previously, she directed the Digital Society Institute at the European School of Management and Technology in Berlin. From 2018 to 2021, she served as Estonia's Ambassador for Cyber Diplomacy advocating for international law and norms in cyberspace. Before this, she headed the Cyber Policy Coordination Unit at the European External Action Service, where she advanced EU external cyber relations, led the development of the EU Cyber Diplomacy strategies and initiated EU cyber capacity-building programs. In 2011, she worked at NATO, crafting its second Cyber Defence Policy. She led the development of the first Estonian Cybersecurity Strategy after 2007 coordinated cyber-attacks against the country.

The Origins of Cyber Diplomacy: Great Power Cyber Competition and Rapprochement in the United Nations 1998–2021

Michele Markoff

Most cyber diplomats view 2021 as an important milestone in an arduous 24-year diplomatic process in which Russia, the United States and China competed to impose very different visions of cyberspace on the world. Although Russia and China have continued to contest the outcome, the United Nations General Assembly in 2021 unanimously adopted the first normative framework to guide state conduct in cyberspace. Developed between 1998 and 2021 through a series of six United Nations-sponsored Groups of Governmental Experts (UNGGEs), this precedent-setting agreement is composed of three elements. It affirms the applicability of international law to state actions in cyberspace with the intention of safeguarding civilians and civilian infrastructures. It underscores the utility of confidence-building measures (CBMs), Cold War tools designed to create greater predictability of state actions in cyberspace. It adopts unique voluntary measures, often termed 'norms', designed to diminish the prospect of conflict

in cyberspace when states operate offensively below the threshold of the use of force during peacetime. Taken together, these elements constitute the only normative framework on which all UN member states have agreed thus far to maintain cyberspace stability and prevent the overt outbreak of nation-state cyber conflict or its escalation to physical conflict.

These measures have gained an important foothold in the global consciousness as the 'Framework of Responsible State Behavior in Cyberspace'. All UN member states have pledged to be guided by the Framework and agreed that it is the basis from which any additional steps to reduce risk from information technology (IT) should originate.

The Framework has created a rallying point for responsible states willing to use it to judge and call out unacceptable cyber behaviour. Some have also used the norms to justify imposing consequences such as sanctions or indictments on perpetrators. As yet, no state-on-state cyber incident has breached the threshold of the use of force, indicating at least indirectly the Framework's influence, though no metric exists to measure its effect.

While the outcome was unanimous, the countries driving this process— Russia, China and the United States—have different motivations and end goals. This paper outlines key elements of the process of competition and agreement that shaped the outcomes that brought together all countries in an effort to prevent cyber conflict.

The United Nations: An unlikely venue

In 1998, the UN would have been voted the institution least likely to be an instrument of US foreign policy by most policymakers. If not for the tenacity of Russian policymakers, who understood their weakness in the competitive technology revolution, the UN would never have evolved into the venue for discussions of cybersecurity.

Since the Soviet Union's collapse in 1991, Russia was considered a failed state, arms control efforts were moribund, and the US attitude towards the UN was one of benign oversight to ensure the institution stayed within well-defined lanes. Russia had little leverage to get the United States to engage bilaterally in discussions of a technology threat that had yet to materialise. In 1998, Russia's strategy aimed to pressure the United States in the UN to agree to controls on a technology where it feared it could not effectively compete. Bringing its case to the UN would allow it to enlist the support of political allies. That way, it could force the United States to engage diplomatically.

Russia bet correctly that few states would oppose its little 'anti-war' resolution on a poorly understood issue that was aimed at unseen armaments composed of computer technology. Russia wanted an agreement to ban the development, deployment and use by states of what it termed 'information weapons', a catch-all phrase that covers the spectrum of information operations to include physical as well as electronic weapons and, interestingly, content such as propaganda and influence operations.

The US government was predictably dismissive of Russian proposals. The notion that the United States would simply negotiate technology options away with a failed adversary was not on the table. The US Department of Defense (DoD) had said nothing publicly on the weaponisation of IT. US and Russian governments, working on IT, were driven by different imperatives. 'Cybersecurity' efforts by the US government were focused on defending data and systems while Russia pursued 'information security' technology to disrupt systems and spread information in support of state security aims. DoD feared public sensitivity over military uses of IT. The World Wide Web was less than a decade old; the beguiling promise of computer technology and the vision of a world of manifest destiny was being propagated. Acknowledgement of offensive development of IT could be opposed strongly.

Nor was it clear how arms control constraints might be devised to capture offensive uses of a technology that was becoming ubiquitous. Mass destructive technologies, such as chemical, biological, radiological or nuclear (CBRN) ones, were so destructive that the international community pronounced them unusable, and they required precursors possessed only by states, therefore nations could agree to ban them totally.

IT was the opposite. It offered negligible technical barriers to development, had low cost of entry, and offered significant leverage for modest effort: yielding an equal opportunity tool swiftly dominated by anyone who could think of a purpose for it. Early concerns about misuse pertained to misuse that was criminal in nature. None of this was thought to be state-based.

Unlike weapons of mass destruction (WMDs), IT was neither owned nor controlled by governments. To call it 'dual use' was an understatement. It was used by everyone, could be weaponised by anyone and featured no external observables or threshold barriers to prevent anyone from using it destructively. Nor could perpetrators be identified in a timely manner. As an offensive tool, IT potentially was usable across a spectrum of violence from annoying pings to cascading centre-of-gravity infrastructure failures as society became more cyber-dependent. The proposition that offensive use of IT could be banned or controlled through state agreement was not and is not credible.

The United States opposed Russian UN proposals for a decade, but it was forced to engage, if only to prevent these proposals from gaining a serious foothold in the UN. Russia remained patient, renewing its resolution annually and making it more palatable to the Western European and other likeminded states so that it would pass annually.

The US view remained that IT needed to be secured and defended, not banned. To counter the Russian contention that technology bans were the only way to ensure cybersecurity, the United States underscored the necessity for all nations to build capacity to defend themselves against attacks through cyberspace. This remains the heart of the US approach to cybersecurity capacity building.

A theory of cyber-conflict prevention

A single event challenged the US attitude. The Russian 2007 cyberattack on Estonian government networks in response to a political dispute over the relocation of a Russian Second World War memorial suddenly focused US attention on what was the first state-on-state cyberattack. Russia demonstrated the potential impact a cyberattack could have on national security as societal dependence on networked infrastructure became pervasive.

The Estonia attack prompted a US reevaluation of Russia's use of cyber power and prompted new US interest in engaging diplomatically on the subject of state-sponsored cyberattacks. Estonia had come close to petitioning the North Atlantic Council to discuss invoking Article V of the Washington Treaty. This was not the touted 'cyber Pearl Harbor' for the United States by any stretch, but it could no longer be argued that cyber warfare was not a foreign policy issue and didn't need a strategy.

An organising concept was needed. The attributes of IT as a weapon were novel and, as demonstrated against Estonia, impactful in meaningful ways. There were no rules of state conduct for 'information weapons'. The 'weapons' could be used at any time and cross the world in unpredictable ways on private sector networks, through servers in dozens of unwitting countries with no notice even in the absence of active hostilities, yet not breach the threshold of the use of force. This was unprecedented.

Yet if limiting the technology was neither desirable nor feasible, risks to US security could conceivably be managed through diplomacy by trying to limit the effects of state use. This idea propelled development of a position to counter Russia and to coalesce the international community around the objective of preventing and managing the risk of cyber conflict by employing familiar political–military concepts.

For example, the United States accepts the constraints of international humanitarian law (IHL) on its weapons use during armed conflict as binding. Couldn't state use of IT be declared subject to the same rules of warfare as any other use of armed force? This would in theory safeguard civilian objects from cyberattacks in armed conflict. The United States could propose that international law be affirmed by all states to apply to offensive state use of cyber tools.

Another unique attribute of IT was that malicious cyber tools have no external observables. Thus, accurate prediction of either the identities or the intentions of adversaries would be both elusive and essential. Finding an off-ramp from conflict or escalation by ensuring real-time communication with adversary policymakers would be critical, but how? Cables and demarches would prove too slow.

The Cold War art of confidence-building measures could provide such a tool: voluntary, mutual measures could be negotiated to prevent misperception, permit predictability and facilitate communication. The UN Office of Disarmament Affairs (UNODA) describes them this way: 'Confidence-building measures (CBMs) are planned procedures to prevent hostilities, to avert escalation, to reduce military tension, and to build

mutual trust between countries. They have been applied since the dawn of civilisation, on all continents.'

For example, the lack of external observables of cyber tools could be mitigated by exchanges of 'white papers'. These are doctrinal documents that articulate a state's intentions with regard to a form of warfare. Other efforts require all parties to effect them cooperatively. The most famous example is the 'hotline' that maintains a contact link between Washington and the Kremlin. The final type of measure involves agreement on measures of mutual restraint. These types of measures would play an important role in 2015, when they would be called 'norms'.

The first two strategies—affirming the applicability of international law to cyber activities and the adoption of CBMs to prevent conflict through enhanced predictability and communication—became the key pillars of the US negotiating position contesting Russia's call for a cyber arms control treaty. It was this approach that the United States presented at the 2009–2010 Russia-initiated UNGGE.

Towards a framework of responsible state behaviour

It had taken a decade for the United States to respond substantively to Russia's 1998 cyber treaty proposal. The response outlined above came in the form of a 16-page US submission to the 2009–2010 UNGGE, proposed by Russia and convened for a year at 15 states.

Whether delighted or relieved, the Russian chair welcomed the US paper and unexpectedly adopted it as his own. The political environment was propitious. The new Obama administration had called for a 'reset' with Russia and the atmosphere was upbeat. None of the elements of the US submission seemed controversial during the year-long negotiation until the final week, when China seemed to suddenly take notice. Indeed, the US position was attractive because the approach was familiar even if the subject matter was not. As UN member states, acceptance of the Charter and the application of international law to armed conflict, even with a new technology, was legally familiar, especially for members of the Permanent Five (P5). The role of CBMs in preventing conflict was well known during the Cold War.

China made it clear that it wanted none of this, rejecting both the applicability of international law (IT was 'unique' and needed 'new' rules) and the notion of CBMs (China was not a party to CBMs during the Cold War; that was a US–Russia thing, it said). China had simply been a 'free rider', apparently monitoring the situation to ensure absolutely nothing happened. It was represented by Fang Binxing, otherwise known as the 'Father of China's Great Firewall', who never uttered a word, content to play computer games during meetings. That changed with the apparently alarming prospect that the United States and Russia had found some common ground and were moving with the others towards an agreement.

China suddenly dispatched an idiomatic English-speaking diplomat to contain the damage. Due to Russia's staunch

defence of the report, he only managed to excise 12 pages of the detailed international law applicability explanation from the proposed report. This left an unprecedented four-page consensus report with a commitment to further discussion of international law and other 'norms, rules and principles' of state behaviour, and CBMs as the now agreed road map for future cyber discussions in what was the first unanimous UNGGE report, thus setting the stage for the coming decade.

Shanghai Cooperation Organization Code of Conduct

China would not be caught off guard again. Nor would it rely solely on Russia to protect its interests, especially in the context of the ongoing US–Russia reset. But the reasons for China's actions were unclear. While Russia pressed for a binding treaty on cyberspace, China stood silently in clear opposition to the applicability of existing international law to state activities in cyberspace. Its silence left the clear impression that it simply did not want to be constrained, even by IHL.

In late September 2011, China, Russia, Uzbekistan and Tajikistan, all members of the Shanghai Cooperation Organization (SCO), asked formally to table a document for discussion in the UN First Committee where the cyber discussions were being held. Many documents are table-dropped in the UN during ongoing negotiations with little fanfare. Most of those formally tabled are draft resolutions. This was different.

China, using the SCO, was testing the water with its alternative view of cyber norms and rules. This effort built upon an unnoticed 2009 SCO mutual cyber defence agreement. In a letter to the UN on 12 September 2011, the SCO stated that it had 'jointly elaborated an international code of conduct … with the aim of achieving … consensus on international norms and rules guiding the behavior of States in the information space' (UN Doc A/66/359). This Code was meant to challenge the US proposal to affirm the applicability of international law in the upcoming UNGGE.

The 'International Code of Conduct for Information Security' received a lukewarm reception when the next Russia-proposed GGE commenced in 2012. There was nothing particularly new about it except for its subject. It was an expansion of the Five Principles of Peaceful Coexistence that had been the basis of Chinese foreign policy since 1954, reworked to apply to IT and the internet. It now made clear that freedom online was subject to domestic law and that a nation's information space is sovereign territory. These authoritarian principles remain at the heart of Chinese and Russian policy today. It had few takers. The Code of Conduct gained no traction during the negotiations.

The mandate of the UNGGE that began in 2012–13 was to further discuss applying international law to state cyber conduct and to elaborate CBMs. Russia tabled its own detailed paper on international law. When the chair's draft of the report emerged, it was unprecedented in its recommendations (UN Doc A/68/98). Statements affirmed that international law applies to state cyber use, that sovereignty applies over

physical IT infrastructure in their country (not over content), and that cybersecurity cannot be imposed nationally at the expense of human rights guaranteed under the United Nations Declaration of Human Rights (UNDHR).

Other states' experts drafted observations on how international law should apply, adding to the deepening record of states' views. Additional statements mandated that states must meet their obligations regarding internationally wrongful acts attributable to them; they must not use proxies to commit wrongful acts; and they should ensure that their territories are not used by non-state actors for criminal misuse of IT.

There was one problem. Throughout the negotiation, China stood silently by, occasionally protesting the discussions on international law. All other state experts worked with a sense of common purpose, even those for whom the implications of IT remained unfamiliar and national positions unformed.

One intervention by China resonated unexpectedly as it defended its resistance to affirming the applicability of international law. Why was such an affirmation useful when none of the cyber incidents that states perpetrated breached the threshold of the use of force? None of these disruptions constituted armed conflict. What, China asked, are the rules that apply every day during peacetime?

China had a point. What constitutes armed force in cyberspace was and remains an open question for many states. The United States has stated that a 'use of cyber force' definition likely required a component of lethal effects. Below the threshold, the responses available under international law were limited and

lacked any deterrent effect. More importantly, there was no agreed standard of conduct against which states could be judged if an information weapon did great damage below the threshold of the use of force anywhere in the world during peacetime. What acts warranted a response? What could the responses be?

Notwithstanding this, 14 of the 15 states agreed to the final 2013 report text early in the last week. Despite the souring 'reset' with Russia, it remained on board. China would not budge. It would not accept the sentence beginning 'International law applies…'. The success of this new GGE, which required unanimity to issue a report, hinged on getting China to change its position on this key issue.

Never discount the importance of luck when it comes to diplomacy. President Xi had just arrived in California on 7 June 2013 for a two-day meeting with Obama on his way to South America. This was the penultimate day of the UN experts group negotiation. The prospect that there would be no agreement the next day after such breakthrough work was very real. As a last resort, it was casually noted to China's negotiator that a UN Security Council member being the only nation to reject the applicability of international law to cyberspace would likely merit a front-page story critical of President Xi. That was enough to clinch agreement on the pivotal 2012–13 GGE report, however reluctant. China spent the next decade, though, trying to walk that concession back.

Peacetime norms

Back in Washington, China's question regarding what rules of state conduct should prevail below the threshold of the use of force resonated. The question was put to an inter-agency lawyers' group co-chaired by the National Security Council and the State Department: Could principles be developed for state cyber conduct during peacetime where conflict was being waged in a grey zone: neither peace nor war? Could risk to civilians and civilian infrastructures from cyber disruption be limited by negotiating norms of conduct?

Creating new international norms is a tedious business. They bind you as well as your adversaries, and thus are not to be entered into lightly. The lawyers' process did produce three non-binding normative proposals to which the United States was willing to obligate itself.

Two of the norms seek voluntary non-binding international restraint against specific targets. The first precludes the attacking of critical infrastructures that provide services to the public and the second asks states to forswear attacks on CERTs and using theirs for offensive purposes. The final normative statement admonishes states to respond to requests for assistance, especially when the requests are to mitigate malicious activity aimed at the critical infrastructure of one country emanating from the territory of the other.

The success of the 2013 report fostered expectations that the next UNGGE in 2014–15 could be even more productive. After years of indifference, there was lobbying among UN member

states to participate in the next group. The UNODA agreed to expand the group slightly. The next group commenced with an expanded membership of 20 member states. Increasing the number meant the road to consensus would be bumpier, as many of these states had never participated in any cyber discussion. The other problem was that the US–Russian 'reset' suffered a strong blow with Russia's annexation of Crimea. Even relationships between long-time US and Russian counterparts were tense.

Yet progress towards yet another expert report was workmanlike and detailed on CBMs and cybersecurity capacity building. Language to strengthen the application of international law gained no ground as China refused to allow even a repetition of the 2013 language.

It was the US response to China's rhetorical question from 2013 regarding what rules apply to state conduct below the threshold of the use of force that attracted the most support. Tabling the three norms it had developed was a calculated risk. It could have opened the floodgates and prompted calls for binding agreements. Had it done so, the United States could always have broken consensus.

The US normative proposals were welcomed and adopted with some edits but maintained their original intent. The process did inspire other proposals, and the group reported on 11 norms in all. Several were hortatory; others embodied statements made in earlier reports that, like the US statements, forswore certain actions (UN Doc A/70/174. Para 13).

The norms were adopted, clearly labelled 'voluntary and non-binding'. While this has been a source of criticism, the UN experts' groups had a mandate to explore options without formal agreement. While these norms ultimately became political commitments of all UN member states after UNGA votes affirming that all states would be 'guided by' them, there was no appetite to make them binding on an issue so unfamiliar. But the idea that cyber norms were useful was now firmly established. A sentence of the report underscored the purpose of the norms: 'Norms reflect the expectations of the international community, set standards for responsible State behavior and allow the international community to assess the activities and intentions of States' (para. 10).

Evaluating state conduct

An agreed framework of expectations for state cyber behaviour was desperately needed by then. The years of the 2014–15 UN experts' group had featured a continuum of splashy public cyber incidents: the Sony Pictures hack (DPRK), the Anthem and OPM hacks (China), the Black Energy attack on the Ukrainian power grid (Russia). The world had gone from hacktivists and 'white-hat' hackers to the use of state power to degrade and disrupt cyber infrastructure critical to the safe operations of civilian infrastructure.

Suddenly, confusion reigned in the US government regarding exactly how to respond and what was a legal response. Some White House statements underscored the 'serious' national security significance of the Sony Pictures attack. A few months

later, China's hack of the Office of Personnel Management (OPM) database, exposing the personal data of four million government employees, was treated as ho-hum. In neither case did the United States make more than disgruntled statements in response.

This policy uncertainty in response to disruptive cyber incidents highlighted the absence of an effective decision-making process by which to evaluate the true national security significance of any particular cyber incident. Nor was there a thoughtful or orderly process by which to decide what to do about them. It would soon become obvious with NotPetya (Russia) and Wannacry (DPRK) in 2017 and the Russian attempts to interfere in the 2016 election that future destructive incidents would ignore borders and affect many US allies, yet not constitute a use of force that would allow a destructive military response.

To the extent that the United States had prepared for any significant cyberattack, it anticipated the often touted 'cyber Pearl Harbor', that is, destruction with strategic effect and likely above the threshold of the use of force. Indeed, agreed declaratory policy reserved to the president the right to use any instrument of national power in response to a cyberattack. This statement allowed that a cyberattack could be met with kinetic weapons rather than in kind. This responded to a Russian statement promulgated years earlier declaring that a cyberattack on Russia would be treated as an attack by WMDs. But none of those well-understood deterrent conditions applied. Kinetic instruments were only useful if the incidents breached the threshold of the use of force. At the same time,

retaliatory cyber responses were not an option because they were thought then to be potentially escalatory and not well controlled. An understanding of response options for grey zone cyberattacks was severely lacking.

The cumulative recommendations of the UN experts' reports up to and including 2015 filled an important international vacuum: the need for an internationally shared yardstick by which to judge unacceptable state conduct in cyberspace both in armed conflict and in the so-called grey space. Such a framework could be used as a guide around which to coalesce likeminded states that wanted to preserve stability in cyberspace through responsible action as well as to understand the conditions under which an individual or collective response to malicious actions would be warranted. Informally christened the 'Framework of Responsible State Behavior', the norms, supported by international law and a plethora of CBMs, constituted the only internationally agreed foundation of acceptable state behaviour.

Patience required

Diplomatically, the UN work was still incomplete. A concluding report was needed that catalogued all the recommended norms and agreements from three reports in one place and explained plainly what they meant and how member states should implement them. No new ground needed to be broken. Nevertheless, that task would take four more years as the weight of Russia's annexation of Crimea and Western responses weighed heavily.

The failure of the next UNGGE to reach consensus in 2016–17 was predictable. The subsequent eulogies and autopsies of the process were legion. The pretext for the collapse was the attempt to agree on affirmation of Article 51—the right to self-defence—of the UN Charter. This was another bridge too far for China. The subsequent declarations of the death of the applicability of international law issued by many think tanks were hyperbolic. This was all unwarranted. There was no urgent mandate to break new ground: all the United States wanted was an artful summation and a road map for member states to follow to implement the Framework.

The lack of unanimity simply meant that no new UNGGE report would be issued. There would be no formal record of the regression, and any future experts' group would revert to the last consensus report of 2015 as a starting point. An undesirable digression, but no harm, no foul. An up-cycle would eventually occur.

Reviving the undead and cloning

With no improvement in the political climate, the hiatus in cyber discussions lasted until 2019, when Russia tabled a draft resolution proposing a new UNGGE (A/C. 1/73/L.27/Rev.1). The draft was a regression, disavowing all prior common ground and agreed norms. The substance focused on legitimising sovereign control of the internet and regulating control of the domestic online environment. While purporting to support prior agreements, it cherry-picked elements of the 2013 and 2015 consensus reports and distorted their meaning.

In an unparalleled act of diplomatic one-upmanship, China joined with Russia to propose making the group an 'Open Ended Working Group' (OEWG) with inclusive membership comprising all 193 UN states, rather the prior 20. Russia lobbied forcefully: inclusiveness for the first time; a chance to reopen all the normative statements most had had no part in drafting. Such arguments swayed many of the nonaligned states, which smarted from the fact that they still stood on the wrong side of the digital divide.

The Russian resolution passed despite opposition from the United States and other states that supported the traditional UNGGE process, constituting a new and serious threat to prior agreements. Rather than concluding a report, the United States would have to play defence to prevent any report issued by the new OEWG did not disavow the prior consensus reports, or it would have to be blocked.

Moreover, the United States felt that the destructive intent of the OEWG could not go unchallenged. The unprecedented solution was for the United States to sponsor the original resolution and call for one last GGE to proceed in competition with the Russian effort. The US goal: to gather together all the unanimous text and recommendations from the prior consensus reports, explain them and offer a road map for adoption by member states in a single report.

It was an Alice in Wonderland moment. If the UNGA voted both resolutions through, the two groups would negotiate towards conflicting ends in parallel for a year, and conclude within days of one another. The last point was critical. Both groups would operate on the basis of consensus. In essence, the success of

one would be hostage to the success of the other. Each side had to be able to read the handwriting on the wall before they voted. Of course, someone would have to go first.

Given the polarisation of the pro-Russia OEWG and democratic like-minded UNGGE, it seemed less like an insurance policy and more like a suicide pact. Perversely, Russia, China and the United States (among others) would be members of both groups! If Russia blocked consensus in the GGE, the United States and likeminded states would be sure to block consensus in the OEWG. It would be a matter of trust and crossed fingers.

The vote on both resolutions occurred on November 8, 2018. The U.S.-sponsored former Russian resolution passed: 153 in favor, 11 against, and 9 abstentions, a success. The new Russian OEWG resolution also passed: 104 in favor, 50 against and 20 abstentions, less of a success, but still a go. Ultimately, COVID would intervene to interrupt even the best laid plans.

OEWG vs GGE 2020–21

The success of these two competing endeavours would rest squarely on the skilled chairmanship of two career diplomats, Swiss and Brazilian. The United States saw the job of the Swiss in chairing the OEWG as being to bring all 193 member states to support the cumulative consensus reports of the UNGGEs that they had voted for in the UNGA and to recommit to them unanimously in a new report without unacceptable revisions. In 2020, no one would have taken a bet on that outcome. Russia's objective was the opposite. It wanted the OEWG to revise prior

recommendations to legitimise the authoritarian state-centric approach it and its allies preferred, and endorse a binding treaty in which to enshrine it.

The Brazilian chair of the new UNGGE had no less important a task: preside over the drafting of an explanatory text of recommendations from three consensus UNGGEs with the unanimous support of 25 states, demonstrating how all 193 UN member states could implement them. Oh, and all of this with Russia and China potentially as spoilers.

Adding to the challenge, COVID meant that the chairs had to manage this process in fits and starts, all on unpredictable online formats with live interpretation in the six official UN languages.

UN meetings of the 193 on issues of great interest most closely resemble the Roman Coliseum, where designated gladiators act as proxies for groups of states in the stands. The OEWG was a prime example. Notable was the fifth column recruited by Russia consisting of Iran, Cuba, Syria, Venezuela, Nicaragua, Egypt and South Africa, voicing a litany of anti-Western attacks on a rotating basis. The prevalent theme was that the prior consensus experts should be abandoned in favour of whatever the OEWG was able to agree to now that everyone was participating.

To Russia's disappointment, a majority of the participating states voiced strong support for the Framework as represented in the 2015 UNGGE report as the foundation for any future OEWG report. The decisive position on that issue was voiced by China. China stated that any normative language should be

drawn verbatim from prior consensus UN experts' reports, and cited as such. In an instant, the OEWG was transformed from being a wholesale challenge to the Framework to affirming and enshrining it.

Despite the formal policy 'alliance' between Russia and China, the latter was staking out a much more independent path. If there were no further attempts to extend common understandings on international law, China would not contest the prior UNGGE consensus reports. The significance of this cannot be overstated. Most of the 132 nations that comprise the so-called group of non-aligned would follow China's lead. Russia and its closest allies were now isolated. Would they join consensus on a more conventional OEWG report?

The 6th UNGGE, working in parallel at 25 states, resembled a well-oiled collaborative machine in comparison. The task of compiling the years of consensus recommendations and making them intelligible fell to experienced scribes, battle-hardened from prior experts' groups. They edited the diplomat–experts with finesse and sensitivity. Despite the tension and the duelling resolutions, the decades-long familiarity of the Russian, US and Chinese experts allowed the careful wordsmithing to proceed with consideration and respect. In fact, amusingly, final disagreements on English wording were between Russia and China and put to the United States to help resolve.

The carefully timed ending for both groups was upended by the pandemic. Russia was scheduled to vote on the UNGGE report first, allowing the United States to decide how to vote on the OEWG report after. That was no longer the case. The

United States would vote on the OEWG report first in March, almost two months before the UNGGE would conclude.

China had ensured that the Framework survived intact in the OEWG report. But the active participation of more than 60 other states resulted in a smorgasbord of inputs ranging from clueless to hostile and destructive. Were they included in a final report, the United States would have had to break consensus. That would in turn doom the UNGGE report when it was so close to achieving the US goal of an explanation and roadmap to implementation of the Framework.

In a diplomatically impressive sleight of procedure, the Swiss chair of the OEWG proposed quite simply that only consensus statements would comprise the formal report and all else would be put into a 'Chair's Summary' and be available for additional discussion in the future. Despite some grumbling, that is what occurred.

The United States voted 'yes' in March. The OEWG ended in a consensus that affirmed the Framework. But there was nothing to guarantee that Russia would follow suit in May in the UNGGE or what price it might try to exact to do so.

Ransomware as serendipity

What happened next is a case study in the influence of political context on diplomatic outcomes. On 7 May 2021, Colonial Pipeline, an oil and gas transport company, shut down operations, its billing servers held hostage to 'Darkside,' a criminal ransomware group operating from Russian territory. It

was declared a national emergency by the Biden White House, and the delivery of gasoline and jet fuel came to a halt on the Eastern seaboard a week. This followed the April discovery of Solar Winds, a highly destructive Russian malware that affected 18,000 US machines. Finding an effective way to respond to these destructive cyber incidents was the key focus in the Biden Administration.

On 15 April, Joe Biden announced sanctions against Russian technology companies in response to Solar Winds malware, indicating that Russian intelligence was likely behind both Solar Winds and cyber interference in the 2020 US presidential election. He stated he had spoken to Vladimir Putin, and might have gone further in imposing consequences but would prefer to improve the relationship. The future of the UNGGE report suddenly looked bleak.

The Colonial Pipeline ransomware hack was followed a few days later by REevil, on a Brazilian-owned meatpacking enterprise in the United States. These cases were attributed to Russian-speaking/located criminal gangs, not the Russian government. This propelled the Biden Administration to renew a bilateral cyber dialogue with Russia that had been cancelled since the annexation of Crimea (the last meeting had actually been in 2016). On 13 May 2021, appearing to lean on the UNGGE Framework's due diligence norm, President Biden stated, 'We have been in direct communication with Moscow about the

imperative for responsible countries to take decisive action against these ransomware networks'.[13]

The Russians seemed pleased to have the discussions, as they had often pressed to restart bilateral cyber talks and for a few short weeks cooperation overcame the frozen relationship, even though Russia seemed genuinely confused by the US concern with ransomware that Russia dismissed as petty crime, in contrast to its own preoccupation with state-sponsored cyber conflict.

This tense dialogue began yielding results and would lead to the first summit between Presidents Biden and Putin in Geneva on 16 June. They agreed there to restart cybersecurity and arms control talks and send their ambassadors back to capitals. It appeared that communications, principles for action and processes based on the Framework were in play.

In the midst of these heightened expectations for a reinvigorated cyber dialogue on cyberspace issues, the final week of the UNGGE negotiations took place. Had this slight thaw not occurred at this exact moment, it is anyone's guess what the outcome might have been. As it was, on 28 May an initial agreed draft was issued and on 28 June a final UNGGE report draft was tabled by the chair, to which all expert members agreed. The United States had accomplished what it set out to do: issue a clear concluding document that summed

[13] The White House. (2021, May 13). *Remarks by President Biden on the Colonial Pipeline incident*. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/

up and explained the consensus of the international community regarding the framework of responsible behaviour by states in cyberspace.

Post-mortem and look ahead

The UNGGEs in 2010, 2014, 2016 and 2021 were discussions on a novel topic that produced certain consensus understandings in the hope that diplomacy could help to prevent the risk of war in cyberspace through the use of well-understood tools: the affirmation of international law, and the implementation of CBMs designed to prevent escalation of cyber conflict. The norms were designed to be a voluntary standard of conduct for states to observe during peacetime in the so-called grey space to prevent breaches of the threshold of force. This foundation has been embraced by the entire UN membership repeatedly, even though it can be debated whether all states observe their political commitments.

The short period of rapprochement in 2021 allowed the final concluding agreements of the last UNGGE and the first competing OEWG to be successful. The hotly debated issue of what comes next—formally raised in expert consensus reports as the question of what sort of inclusive permanent mechanism should be established in the UN First Committee to discuss these issues—is simmering, and will be hotly contested.

Michele Markoff

Acting Deputy Assistant Secretary for International Cyberspace Security in the Bureau of Cyberspace and Digital Policy

Michele Markoff is the Acting Deputy Assistant Secretary for International Cyberspace Security in the Bureau of Cyberspace and Digital Policy. Since 1998 Michele has been the senior State Department subject matter expert overseeing the development and implementation of foreign policy initiatives on cyberspace issues. She helps to coordinate United States policy on the spectrum of cyber-related policy issues across the Department, develops diplomatic strategies to encourage states to join the United States in taking steps to protect their critical networks and to cooperate internationally to enhance and preserve global cyber stability. She implements those strategies through negotiations in a wide variety of venues. Her initiative led to the successful completion of the first ever bilateral agreement on confidence-building in cyber space between the United State and the Russian Federation, announced in June, 2013. Michele also has been the United States Government Expert on five Groups of UN Government Experts (2005, 2010, 2013, 2015, 2016) devoted to international security cyber issues. The last three GGEs led to landmark consensus reports regarding norms for state activity in cyberspace. Ms. Markoff is also the architect of two agreements on cyber confidence-building measures in the Organization of Security Cooperation in Europe, and a similar initiative in the ASEAN Regional Forum. Ms. Markoff was trained as an expert in Russian and Chinese military affairs and decision-making and spent the first half of her career in a variety of strategic nuclear

arms control-related posts, among them as State Department Advisor and then Executive Secretary to the START I Talks; later as Senior Policy Advisor and Director of the U.S. Arms Control and Disarmament Agency's Policy Planning Group. Ms. Markoff has a B.A. in International Relations from Reed College, an M.A. in International Relations and an M.Phil.in Political Science from Yale University, and a M.Sc. in National Security Strategy from the National War College of the United States. She also attended high school in the former Soviet Union and attended the Chinese University of Hong Kong.

Part 2

REGIONAL AND MULTILATERAL PERSPECTIVES

European Cyber Policy and Cyber Diplomacy

Manon Le Blanc and Andrea Salvi

Introduction

In an era where technology underpins every aspect of human life, cyberspace has emerged as a critical domain. Cyberspace enables our communication, the functioning of our critical infrastructure such as hospitals, banks, our transport, and is a key driver of business all around the world. It functions as both an enabler and an amplifier of human interaction, reflecting geopolitical conflict and competition in cyberspace with tangible implications for the physical world. In a time where some states are increasingly aggressive, including in cyberspace, cyber became a tool of statecraft. Authoritarian states are advancing a vision of cyberspace based on state-control, which has profound implications for the global governance of cyberspace, for international security as well as for the rights and freedoms of millions of people.

Recognizing the potential impact of an authoritarian control-driven vision of cyberspace, the European Union (EU) has developed a set of diplomatic activities and cyber diplomacy policy to promote the EU vision of a global, open, free, stable and secure cyberspace, and counter malicious state behaviour in cyberspace. Reckoning the need for international cooperation to address global challenges, the EU has

positioned itself at the forefront of shaping its cyber ecosystem and advancing cyber diplomacy as an area of activities. Particularly, the EU's unique institutional framework, value-driven policies and robust economic and regulatory foundation define its strategic approach and enable it to contribute to peace, security and stability in cyberspace.

Cyber as a field of diplomacy

Cyber ecosystems are vast, complex and dynamic environments comprising technologies, legislation, policies, and a multitude of actors, including public and private entities, the technical community, civil society, as well as end users. Rapid technological advancements, comprehensive regulatory and policy frameworks, the EU's role as the world's largest trading bloc and the diverse strategic national security approaches of its 27 Member States shape the EU's ecosystem. The global context—marked by power dynamics, technological competition, and differing perspectives between liberal democracies and authoritarian states on Internet governance and digital rights—further influences its efforts.

Cyber diplomacy plays a central role in advancing the EU's vision of cyberspace, in building global partnerships, and countering cyber threats, working in tandem with the EU's internal cybersecurity policies. This essay examines the EU's cyber diplomacy policies and practices, exploring how the EU has established cyber as a field of diplomacy and how cyber issues have become increasingly relevant in geopolitics. It delves into the distinct features of the EU's approach to cyber

diplomacy, its main pillars, and its continued efforts to promote a global, open, free, stable, and secure cyberspace.

The uniqueness of the EU and its approach to cyber diplomacy

The EU's approach to cyber diplomacy is unique due to its institutional structure, value-driven policies and robust regulatory frameworks that harmonize the approaches of its 27 Member States. Unlike individual nation-states, the EU unites diverse national strategies under a shared policy and legal framework, while its Member States retain responsibility for national security. This structure enables the EU to establish a regional baseline for cybersecurity, foster strong solidarity and cooperation among Member States, and present a unified stance on the international stage.

Through collaboration, not only at the level of Member States but also through interservice groups and task forces involving EU institutions, agencies, and bodies, the EU has translated its cooperation into institutional frameworks. These frameworks empower all relevant actors in the cyber ecosystem to contribute to policy development, implementation, and responses to cyber incidents. The Council of the EU[14] serves as the central decision-making body, where national representatives from each Member State negotiate and adopt

[14] The Council of the European Union. (n.d.-b). The Council of the EU is where national ministers from each EU country meet to negotiate and adopt EU laws. https://www.consilium.europa.eu/en/council-eu/.

EU laws, policies, and positions and coordinate operational responses. Within dedicated Council working groups, notably the Horizontal Working Group on Cyber Issues, Member States and EU institutions, agencies, and bodies collaborate to define, implement, and monitor the EU's cyber agenda. Further coordination occurs through dedicated networks, which include Member States' national authorities, such as the EU Computer Security Incident Response Teams (CSIRTs) Network[15] or the EU Cyber Ambassadors Network,[16] and enable as well engagement with the multi-stakeholder community. Additionally, the EU Delegations worldwide play a critical role in aligning Member States' positions, including those reflected in EU statements at the United Nations and other international and regional fora[17].

Four cyber communities

The EU distinguishes four cyber communities: cybersecurity, cybercrime, cyber diplomacy, and cyber defence. Each community has its own policies, initiatives, and mechanisms at technical, operational, and political levels. These communities collaborate with Member States through the Council and

[15] https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/csirts-network

[16] Cyber: EU holds informal meetings of Cyber Ambassadors and Commanders. (n.d.). EEAS. https://www.eeas.europa.eu/eeas/cyber-eu-holds-informal-meetings-cyber-ambassadors-and-commanders_en.

[17] EEAS. (n.d.). EU in the World. https://www.eeas.europa.eu/eeas/eu-world-0_en.

dedicated EU networks, as well as with a broader set of stakeholders. Representatives from these communities also work across sectors to ensure a coordinated and comprehensive approach to EU cyber policy and activities. In this, the European External Action Service (EEAS), the EU's diplomatic service, working closely with the European Commission, plays a pivotal role in developing, facilitating, maintaining and aligning the EU's international relations on cyber.

The development of the EU's cyber diplomacy agenda

To understand the EU's approach to cyber diplomacy, it is essential to examine its strategies and the main pillars of its external actions in this domain. Cyber diplomacy in the EU formally began with the establishment of a dedicated cyber policy taskforce within the European External Action Service (EEAS) in 2012 and the adoption by the European Commission and the High Representative for Foreign Affairs and Security Policy of the first comprehensive EU Cybersecurity Strategy in 2013.[18] From the outset, the EU recognized cyberspace as a domain requiring diplomatic engagement through a specialized policy framework.

[18] European Commission. (2013). Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

Building on the 2013 EU Cybersecurity Strategy, the Council of the European Union issued dedicated conclusions in 2015, emphasizing that the EU and its Member States should address cyber issues through a coherent international cyberspace policy, and further defining the areas of interest for external action. This policy aimed to promote the EU's political, economic, and strategic interests through engagement with key international partners, organizations, civil society, and the private sector. The Council conclusions also outlined for the first time a detailed list of EEAS's priorities, including promoting and protecting human rights in cyberspace, advancing norms of behaviour and the application of existing international law in cyberspace, supporting Internet governance, enhancing EU competitiveness and prosperity, and strengthening cyber capacity-building.

Meanwhile, rapid digital developments and an evolving cyber threat landscape have expanded the scope of EEAS activities in cyber diplomacy. The growing ability and willingness of state actors to engage in malicious cyber activities against the EU, its Member States and partners necessitated an enhanced capacity to prevent, deter and respond to such behaviour. Moreover, the 2017 WannaCry ransomware attack[19] and the NotPetya malware attack[20] underscored the urgent need to counter large-scale cyber incidents and -attacks using all available tools.

[19] Europol (2017). Wannacry ransomware. https://www.europol.europa.eu/wannacry-ransomware.
[20] European Repository of Cyber Incidents. (2023, March 22). Major Cyber incident: NOTPetya - EUREPOC: European Repository of Cyber Incidents. https://eurepoc.eu/publication/major-cyber-incident-notpetya/.

The potential cascading and systemic effects of such attacks on societies, the global economy, and the cyberspace domain itself, led the EU to strengthen its cyber policies and its crisis management framework. Key steps included the 2017 Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU[21] and the 2020 EU Cybersecurity Strategy for the Digital Decade[22] that also included the establishment of an EU Cyber Crisis Blueprint[23] and a cyber crisis taskforce co-chaired by the European Commission's DG CONNECT and the EEAS.

Simultaneously, digital policies gained prominence on the political agenda due to geopolitical and economic factors, a trend further accelerated by the rapid digitalization spurred by the COVID-19 pandemic. This evolution gave rise to digital as a distinct field of EU diplomacy, addressing issues such as developing digital partnerships, the protection of human rights online, the development, governance and secure deployment

[21] European Commission. (2017). Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450.
[22] European Commission. (2020). The EU's cybersecurity strategy for the digital Decade. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.
[23] European Commission. (2017). Blueprint on a coordinated response to large-scale cybersecurity incidents and crises (Council Recommendation No. 2017/C 158/01). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584

of critical technologies, as well as standardisation and Internet governance.

The above developments led to the securitization of cyber diplomacy, as also outlined in the Strategic Compass (2022),[24] crystallising its focus on four core priorities: (1) promoting international peace and security in cyberspace, (2) preventing, deterring, responding to, and defending against the increasing number of malicious cyber activities, (3) strengthening partnerships, and (4) enhancing global cyber resilience.[25] Ever since, the number of cyber-attacks, including in the context of Russia's increasingly aggressive posture, the strategic competition over technologies, and continued discussions on the governance of cyberspace, has put an emphasis on this agenda, leading also to the establishment of a dedicated Division within the EEAS, as well as the appointment of a Coordinator for Cyber Issues.

[24] European Union. (2022, March). The Strategic Compass for Security and Defence. European External Action Service. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

[25] EEAS. (2024). Cyber diplomacy and Cyber defence: EU external action. https://www.eeas.europa.eu/eeas/cyber-diplomacy-and-cyber-defence-eu-external-action_en?utm_source=chatgpt.com.

Promotion of international peace and security in cyberspace

The EU's values-driven approach to cyber diplomacy is firmly rooted in its commitment to multilateralism, the promotion and protection of human rights, democracy, the rule of law, and international cooperation. The EU actively participates in international fora, such as the United Nations, to promote the UN framework for responsible state behaviour in cyberspace, grounded in the application of international law, norms of responsible state behaviour, confidence building measures and capacity-building.[26] It also engages with and within regional organizations, including the Organization for Security and Co-operation in Europe (OSCE),[27] the Organization of American States (OAS),[28] and the ASEAN Regional Forum (ARF)[29] on the development and implementation of cyber confidence-building measures, aimed at enhancing transparency, predictability and cooperation, and reduce misperceptions between states. Through these multilateral and regional

[26] UN. (n.d.) work on Developments in the field of information and telecommunications in the context of international security https://disarmament.unoda.org/ict-security/

[27] EEAS. (2021) The EU and Organization for Security and Co-operation in Europe. EEAS. https://www.eeas.europa.eu/delegations/vienna-international-organisations/osce_en?s=66

[28] The Organization of American States (OAS). (n.d.). Relations with Permanent Observers. https://www.oas.org/en/ser/dia/perm_observers/countries.asp.

[29] The ASEAN Regional Forum https://aseanregionalforum.asean.org/about-arf/

platforms, the EU shares best practices and lessons learnt, contributes to a common understanding of what entails responsible state behaviour, and strengthens international cooperation to actively advance peace, security and stability.

Guided by its commitment to multilateralism and the rule of law, the EU aims to provide a meaningful and legitimate contribution to global peace, stability and security, reinforcing its role as a responsible actor in the global digital landscape. In this vein, the EU, its Member States, and their partners have proposed the creation of a single, permanent, and inclusive UN mechanism to advance responsible state behaviour in cyberspace to follow the completion of the second Open-Ended Working Group (OEWG) on the security of and in the use of information and communications technologies[30] in 2025. This proposal for a UN Programme of Action to Advance Responsible State Behaviour in Cyberspace[31] aims to ensure institutional stability, enabling the international community to focus and build capacities on the practical implementation of the international framework governing state behaviour in

[30] United Nations (2021). *Open-ended working group on information and communication technologies* (established by the UN General Assembly through resolution 75/240 in 2020). https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021.

[31] United Nations General Assembly. (2022). Resolution 77/37: Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security (A/RES/77/37). https://documents.un.org/doc/undoc/gen/n22/737/71/pdf/n2273771.pdf

cyberspace, while also providing a structured approach for further discussions.

In addition, as part of its contribution to implementing the UN framework — which underpins expectations for responsible state behaviour — the EU and its Member States published, in 2024, a Declaration on a Common Understanding of the Application of International Law to Cyberspace.[32] This Declaration reiterates that cyberspace is not a lawless domain and affirms that respect for the UN framework of responsible state behaviour in cyberspace is essential to maintaining international peace, security, and stability.

The EU's values and its objectives for a global, open, free, stable, and secure cyberspace are also reflected in its internal policies and legislation, reflecting a core dimension of the EU's effort to contribute to international peace, security and stability in cyberspace. The EU's regulatory frameworks, such as the General Data Protection Regulation (GDPR)[33] as well as the Directive on measures for a high common level of cybersecurity

[32] Council of the European Union. (2024, November 18). Declaration on a Common Understanding of International Law in Cyberspace (ST-15833-2024-INIT). https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf

[33] The Council of the European Union. (n.d.-b). The General Data Protection Regulation. https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

across the Union (NIS2 Directive)[34] set high standards for data protection, privacy, and security, which directly contribute to the EU's adherence to the UN framework for responsible state behaviour in cyberspace. For example, the NIS2 Directive is further enhancing the requirements for Member States to protect their critical infrastructure by adopting national cybersecurity strategies and establish Computer Security Incident Response Teams (CSIRTs) as well as a European cyber crisis liaison organisation network (EU-CyCLONe).[35] Additionally, the EU Cybersecurity Act,[36] currently under evaluation for possible revision, establishes a framework for EU-wide cybersecurity certification schemes for information and communication technology (ICT) products, services, and processes, and the EU Cyber Resilience Act[37] further harmonizes rules for bringing products with digital elements, hardware or software, to market, including by setting mandatory cybersecurity requirements for manufacturers governing the whole lifecycle of such products. Furthermore, in

[34] European Commission. (2024, November 21). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[35] European Union Agency for Cybersecurity. (n.d.). EU-CYCLOPE: EU Cyber Crisis and Incident Management. https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone

[36] European Union. (2019, April 17). Cybersecurity Act (Regulation (EU) 2019/881). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

[37] European Commission. (2024, December 10). Cyber Resilience Act. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

light of the evolving threat, the 2024 EU Cyber Solidarity Act[38] aims to strengthen EU-wide preparedness, detection and understanding of and resilience and mutual aid against large-scale cyber threats and incidents.

In addition, the EU addresses cybercrime, recognising it as one of the key threats against its citizens and businesses as well as with a potential risk to international security. To prevent and tackle cybercrime, the EU and Member States implement a range of legislative, policy and cooperative measures.[39] These efforts include Europol's European Cybercrime Centre (EC3), which offers operational support and expertise to Member States and international partners in tackling complex cybercrime cases, including ransomware, online fraud, and child exploitation. Internationally, the EU is a strong advocate of the Council of Europe's Budapest Convention on Cybercrime,[40] and has actively contributed to shaping the UN Cybercrime Convention in line with its values. These efforts are essential for maintaining the peace, security and stability in cyberspace, particularly in light of the increasingly blurring cyber threat landscape between state and non-state actors.

---

[38] European Commission. (2024, September 26). The EU Cyber Solidarity Act. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

[39] EU efforts to tackle cybercrime (2024, October 31) https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en

[40] Council of Europe. (2021) Convention on Cybercrime. European Treaty Series No. 185, opened for signature on November 23, 2001, Budapest. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Prevent, deter, respond and defend against malign action

The cyber threat landscape has rapidly evolved in recent years, with state and non-state actors, including cybercriminals and hacktivist groups, increasingly willing and able to conduct malicious cyber activities. This trend has significantly influenced international security, with states leveraging cyber capabilities as a tool of statecraft for malign action, to engage in espionage, target critical infrastructure and influence other nations. This increase in cyber threats and activities has led the EU to continuously navigate its efforts to ensure security, stability, and prosperity for its citizens, while promoting international security and uphold its core values of democracy, human rights, and the rule of law.

The increased cyber threat landscape has also led the EU and its Member States to develop stronger measures to prevent, deter, respond to and defend against malicious behaviour in cyberspace. Reinforced by the 2022 conclusions by the Council on the EU Cyber Posture,[41] the EU has progressively developed a comprehensive approach. Recognising the challenges of deterrence in cyberspace, the EU seeks to implement deterrence across a full spectrum, with measures implemented in a sustained and strategic manner. The approach includes enhancing situational awareness and resilience, imposing costs

[41] The Council of European Union. (2022). *Council conclusions on the development of the European Union's cyber posture*. https://www.consilium.europa.eu/media/56358/st09364-en22.pdf.

on perpetrators, and building global coalitions to strengthen the accountability through collectively condemnation and attribution of breaches and violations of international norms, rules, and principles.

One of the key components of the EU posture is the EU Cyber Diplomacy Toolbox (CDT),[42] which enables the EU and Member States to use the full spectrum of EU tools to encourage cooperation, mitigate threats, and influence the behaviour of perpetrators. The CDT contains a framework that allows for exchange of situational awareness, the design of strategies and measures addressing malicious behaviour in cyberspace, as well as to cooperate with international partners. The CDT has been reviewed in 2023, with the aim to develop a more sustained, tailored, coherent and coordinated EU approach to counter malicious cyber activities, large-scale cybersecurity incidents and an accumulation of malicious activities, as well as to persistent cyber threat actors that target the EU, its Member States and their partners. Since its establishment in 2017, the EU and Member States have implemented numerous measures in response to cyber threats and malicious cyber activities, including private demarches and coordinated EU public messaging to condemn and attribute malicious cyber activities, as well as rapid response, and restrictive measures.[43] To this

[42] The Council of European Union. (2023). *Revised Implementing Guidelines of the Cyber Diplomacy Toolbox*. https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf.

[43] Europol. (2017). *Wannacry ransomware*. https://www.europol.europa.eu/wannacry-ransomware; European

end, the EU adopted in 2019 an autonomous horizontal cyber sanctions regime for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect that constitute an external threat to the Union or its Member States.[44]

Complementing the EU's full-spectrum approach to resilience, response, conflict prevention, cooperation, and stability in cyberspace, in 2022, the EU adopted the EU Policy on Cyber Defence.[45] Driven by the EEAS and European Commission services, in cooperation with the European Defence Agency, the Policy aims to build resilience, enhance coordination among national and EU cyber defence players and between civilian and military cyber efforts, and strengthen the EU's ability to prevent, deter and defend against cyber threats by investments in and use of modern cyber defence capabilities. The EU Policy on Cyber Defence also enables further international cooperation, building on existing security and defence as well as cyber dialogues with partner countries and international

Repository of Cyber Incidents. (2023, March 22). *Major Cyber incident: NOTPetya - EUREPOC: European Repository of Cyber Incidents*. https://eurepoc.eu/publication/major-cyber-incident-notpetya/.

[44] The Council of the European Union. (2019, May 17). Cyberattacks: Council is now able to impose sanctions. https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

[45] European Commission. (2022, November 9). EU Cyber Defense Policy. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642

organisations, notably with the North Atlantic Treaty Organization (NATO).[46]

With these policies and frameworks, the EU approach to deterrence in cyberspace aims to contribute to a global, open, free, stable and secure cyberspace, bridging resilience-building efforts, operational responses, cyber capacity building, and dialogue and cooperation efforts. By using measures ranging from preventive action such as awareness raising to responsive and restrictive measures, the EU has progressively developed a comprehensive full-spectrum approach to addressing cyber threats, forming a coherent system that tackles the multi-layered and varying nature of cyber threats.

Strengthen global partnerships

Given the global nature of cyberspace, the EU cooperates with a broad range of public and private partners to promote international security and stability, exchange best practices and lessons learnt for tackling cyber threats, and make a significant impact on the protection and promotion of a global, open, free, stable, and secure cyberspace. The EU's engagement on cyber issues includes dedicated bilateral and regional cyber dialogues and consultations, practical cooperation to advance stability and security and counter cyber threats, as well as cyber capacity-building initiatives. Cyber issues are integrated into the EU's broader partnership approach, with discussions on

[46] North Atlantic Treaty Organization. (n.d.). NATO. https://www.nato.int/

cyber issues included in political, security, defence, and digital dialogues. These engagements facilitate an exchange of views on cyber policies, cyber threats, and cooperation opportunities in areas such as enhancing resilience, securing critical infrastructure and digital economies, tackling cybercrime, and coordinating positions on cyber in multilateral and regional fora. By advancing cooperation, deepening mutual understanding, and implementing practical efforts, the EU contributes to a global ability to prevent, withstand, and respond to cyber threats, and to keeping cyberspace global, open, free, stable and secure.

Cooperation with international partners takes place across cyber communities. The EEAS, in close cooperation with the European Commission, plays a key role in supporting the development and implementation of policies led by other EU institutions, agencies, and bodies, adding value through its expertise and extensive network for third-country dialogue and cooperation, including its 144 Delegations. For example, the European Union Agency for Cybersecurity (ENISA) provides expertise and support to Member States, EU institutions, and stakeholders on cybersecurity matters,[47] works closely with the EEAS to align its efforts in international cooperation, situational awareness as well as training and exercises involving third country actors. In similar vein, the EEAS works with the *Computer Emergency Response Team for the EU Institutions* (CERT-EU), responsible for enhancing the cybersecurity of EU

[47] The European Union Agency for Cybersecurity (ENISA). (n.d.). *Who we are | ENISA*. https://www.enisa.europa.eu/about-enisa/who-we-are

institutions, bodies, and agencies[48] to respond effectively to external cyber threats.

The EU, recognizing the value of engaging all relevant actors — governments, private sector, civil society, and academia — to ensure an inclusive, effective and sustainable approach to the development of global capacities, strongly supports a multi-stakeholder approach to cooperation in cyberspace. This collaborative approach helps build consensus, promote shared responsibility, and encourage innovation in the field of cybersecurity. By connecting stakeholders from diverse sectors, the EU strengthens the ability of the global community to respond to emerging cyber threats while fostering an environment of cooperation and mutual learning on the global stage.

Acknowledging the critical role of the private sector in cyberspace, the EU fosters particular partnerships with private sector stakeholders on cybersecurity research, development, and innovation, as well as help to shape global governance, build global resilience, and counter malicious behaviour in cyberspace. Notably the EU's Cybersecurity Competence Centre (ECCC)[49] plays an essential role in pooling expertise and resources, strengthening the EU's cybersecurity capacities, and fostering the development of cybersecurity technologies.

[48] CERT-EU – Cybersecurity service for the Union institutions, bodies, offices, and agencies. (n.d.). European Union. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/cert-eu_en

[49] The European Cybersecurity Competence Centre (ECCC). (n.d.). About us. European Cybersecurity Competence Centre and Network. https://cybersecurity-centre.europa.eu/about-us_en

Furthermore, the European Cybersecurity Organisation (ECSO)[50] contributes to the implementation of the EU's unique public-private partnership by bringing together industry, academia, and public authorities on cyber issues.

Enhancing global resilience through cyber capacity building

An important component of the EU's cyber diplomacy policy is strengthening the capacities of partner countries. In order to enable all countries to reap the social, economic, and political benefits of the Internet and the use of technologies, the EU continues to work with its partners to increase global cyber resilience and build capacities to address cyber threats and investigate and prosecute cybercrime. Through targeted support, the EU works to ensure that partner countries develop the necessary legal, technical, and operational frameworks to counteract cyber threats effectively, enhance their digital economies safely and ensure that their state is not a safe-haven for malicious behaviour in cyberspace.

In addition, the EU has increasingly incorporated programmes that enable the development of cyber diplomacy skills, including providing training on cyber diplomacy and, more specifically, on the application of international law in cyberspace. These programmes are designed to not only

[50] ECSO - European Cyber Security Organisation. (n.d.). *Who we are - ECSO*. https://ecs-org.eu/who-we-are/.

bolster technical expertise but to also foster the diplomatic and legal capacities of partner countries. By offering expertise in implementing international norms, rules, principles and standards, the EU supports countries integrate global best practices into their domestic policies, aligning them with international frameworks such as the UN framework of responsible state behaviour in cyberspace.

Answering to the increased need for coordination of cyber capacity building actions, the EU has also strengthened its own coordination efforts, as well as invested in further coordination at the global level. Raising cyber capacity building efforts during every cyber dialogue and consultation, enhancing the coordination with global initiatives such as the Global Forum on Cyber Expertise,[51] as well as the adoption of the EU External Cyber Capacity Building Guidelines[52] and creation of an EU Cyber Capacity Building Board bringing together relevant EU institutional stakeholders, have been important milestones. It demonstrates the EU's increasing commitment to find ways to address the challenge of cyber capacity building coordination at multiple levels, and provides overarching political guidance on the scope, objectives and principles for the EU's international capacity building and cooperation efforts.

[51] Global Forum on Cyber Expertise. (n.d.). Global Forum on Cyber Expertise (GFCE). Retrieved from https://thegfce.org/

[52] Council of the European Union. (2018). EU External Cyber Capacity Building Guidelines (ST-10496-2018-INIT). https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf

Maturing cyber diplomacy in a new age

Despite significant progress, the increasing geopolitical tensions and the interconnectedness of the cyber domain requires the EU to further include cyber considerations into security and defence policies, economic policies, as well as development policies. Over recent years, cyber issues have evolved from technical concerns to strategic geopolitical challenges. Developing comprehensive policies that reflect the interconnectedness of cyber at strategic level, and with other domains such as economic and development policies, is therefore essential, recognizing that geopolitical challenges are inherently multidisciplinary.

The impact of cyber-attacks on critical infrastructures, the rise of cyber espionage, and the proliferation of cyber-enabled influence operations increasing make cyber part of strategic discussions and decision-making processes at the highest levels. Recognizing that actions in cyberspace can have significant implications for national security and international security and stability, the EU works to further integrate cyber considerations into its strategic discourse and overall preparedness and deterrence strategies. This is particularly relevant, taking into account the persistent hybrid campaign, including continuous cyber-attacks, that the EU is facing.

Furthermore, the EU increasingly recognizes the critical importance of secure and resilient digital infrastructure for its economic and geopolitical strategies. To this end, it has developed legislative and policy frameworks, including in

relation to its economic security,[53] that include secure connectivity, digital and data infrastructure, and trusted services. Investments in advanced digital infrastructures, like subsea cables[54] and secure 5G networks,[55] ensure robust and reliable communication channels, reducing vulnerabilities in supply chains. Incorporating a cybersecurity-by-design principle throughout the digital supply chain—from development to deployment—as well as building global partnerships through diplomatic efforts, are essential in promoting interoperability in international markets and ensuring peace, stability and security in cyberspace.

To this end, the EU also recognizes the importance of staying ahead of emerging technologies and evolving threats. Artificial intelligence (AI) and quantum computing for instance present new challenges that require cyber security considerations. The EU AI Act[56] represents the first comprehensive legal framework globally for regulating AI, aiming to promoting safe, ethical, and trustworthy AI applications across the EU. The Act

[53] European Commission. (2023). An EU approach to enhance economic security. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3358
[54] European Commission. (2024). Recommendation on the security and resilience of submarine cable infrastructures. https://digital-strategy.ec.europa.eu/en/library/recommendation-security-and-resilience-submarine-cable-infrastructures
[55] European Commission. (2020). The EU toolbox for 5G security. https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security
[56] European Union. (2024). AI Act, Regulation (EU) 2024/1689. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

categorizes AI systems by risk level—unacceptable, high, limited, and minimal—and establishes standards, particularly for high-risk AI systems used in critical areas like healthcare, education, law enforcement, and public services. To address these risks, the EU should continue to develop a coordinated approach among EU Member States, and to safeguard societies and economies from evolving cyber threats using emerging technologies.

Finally, given the essential role of technologies in economic and social development, as well as in achieving the Sustainable Development Goals (SDGs),[57] development aid also plays a crucial role in advancing global cybersecurity and resilience. The EU's initiatives, such as the EU's Global Gateway,[58] emphasize the integration of cybersecurity into digital transformation projects, ensuring that digital progress does not come at the expense of security and trust. Moreover, the EU has continued to invest in projects[59] that establish solid partnerships and favour the sharing of best practices and technical expertise, as well as empower communities to enhance their digital capabilities while mitigating inherent cyber risks. By embedding cybersecurity considerations into

[57] The Sustainable Development Goals (SDGs), also known as the Global Goals, adopted by the United Nations in 2015, https://www.undp.org/sustainable-development-goals

[58] European Commission. (n.d.). Global Gateway: A stronger Europe in the world. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en

[59] See among others, EU Cyber Direct – European Cyber Diplomacy Initiative (n.d.), https://eucyberdirect.eu/ ; and EU CyberNet (n.d.), https://www.eucybernet.eu/

broader development strategies, the EU ensures that digital infrastructure supports long-term stability and international security. The EU's contributions to the Global Conference on Cyber Capacity Building and its Accra Call[60] also show its commitment to promoting investment in cyber resilience through international and national development agendas, and to promoting cyber capacity building initiatives that are needs-based, addressing the priorities of developing countries.

Way forward

Recognising the evolving geopolitical dynamic and subsequent threat landscape, and building on its cyber diplomacy efforts to date, the EU should continue to further mainstream cyber considerations into broader EU policies. Strengthening the international rules-based order, responding to the threats of our time, building global coalitions and enhancing global cyber resilience in favour of a global, open, stable, and secure cyberspace, are key objectives that can only be achieved through a multidisciplinary approach. In this context, improving coordination and cooperation between relevant communities, both civilian and military, as well as with partners, both public and private, is a prerequisite for effectively tackling the complex and dynamic threat landscape we face today. Strengthening frameworks to share situational awareness and best practices,

[60] Global Conference on Cyber Capacity Building (GC3B). (n.d.). The ACCRA Call for Cyber Resilient Development. GC3B – Global Conference on Cyber Capacity Building. https://gc3b.org/the-accra-call-for-cyber-resilient-development/

build resilience, advance partnerships as well as respond to threats and malicious activities, leveraging the full-spectrum of EU tools, is imperative.

The new European Commission[61] that started on 1 December 2024 has announced a number of new initiatives to enhance the EU's preparedness, strengthen its defence capabilities, and address the increasing number of threats against the Union. In these new strategic documents, including a revised EU Cybersecurity Strategy,[62] the EU will reflect the new reality of threats and challenges, leveraging the EU's institutional framework, values-driven policies, and strong regulatory base on cybersecurity as its unique strengths.

[61] European Commission. (n.d.). The European Commission 2024–2029. https://commission.europa.eu/about/commission-2024-2029_en

[62] The Council of the European Union. (2024). Council Conclusions on the Future of Cybersecurity: Implement and Protect Together (ST-10133-2024-INIT). https://data.consilium.europa.eu/doc/document/ST-10133-2024-INIT/en/pdf

Manon Le Blanc

Coordinator for Cyber Issues and Deputy Head of Hybrid Threats and Cyber Division, European External Action Service (EEAS)

Manon Le Blanc is Coordinator for Cyber Issues and Deputy Head of Hybrid Threats and Cyber Division at the European External Action Service (EEAS) and recognized as one of Europe's top 100 cyber women by the Women4Cyber foundation. Over last years, Manon has shaped the EU's international cyber policies, notably through the development of the EU's Cybersecurity Strategies as well as the EU's framework for a joint diplomatic response ("cyber diplomacy toolbox"). Prior to her posting at the EEAS, Manon held various positions in the Netherlands government. She holds an MsC in Business Administration from the University of Amsterdam.

Dr. Andrea Salvi

Senior Analyst at the EU Institute for Security Studies

Dr. Andrea Salvi served as a Senior Analyst at the EU Institute for Security Studies (EUISS) where he led analyses on cyber and digital issues and directed the EU Cyber Diplomacy Initiative - EU Cyber Direct. Prior to this, he was a Project Officer at the European Commission's Joint Research Centre, overseeing the scientific development of the DRMKC Risk Data Hub. He also worked as a Human Rights Statistics Consultant for the United Nations Mission in South Sudan and held academic roles as a Postdoctoral Research Fellow at Luiss University and a Research

Affiliate at the Center for Research in Leadership, Innovation, and Organisation. Dr. Salvi holds a PhD in Political Science from Trinity College Dublin and three masters' in International Relations, EU Law and Governance, and Cybersecurity. His expertise lies in quantitative methods and computational social sciences, applying innovative data technologies to security and political challenges.

Africa converging on ICT security

Moliehi Makumane

International cybersecurity has been making headlines in Africa. In 2019, South Africa, Kenya, Morocco and Mauritius became the first four African states to have concurrent terms on a Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace. The first Open-Ended Working Group (OEWG) on advancing responsible state behaviour commenced. Intergovernmental negotiations on the security and the use of information and communications technologies (ICT) shifted dramatically away from the limited GGE mandate, while the wide-reaching mandate of the OEWG boomed. Along with such developments, a new lexicon has emerged among African diplomats and policymakers. Use of terms such as 'evidence of attribution', 'peaceful use of cyberspace', 'offensive cyberweapon' and 'cyber for development' in expert statements and national statements grew between 2019 and 2021. The subtext of these terms is often reflective of geopolitical dynamics, which is increasingly a feature of talk about international cybersecurity.

Those who have followed the recent ups and downs of ICT security in Africa know this story: on 3 March 2023, African Union (AU) employees said their work emails and the internet had been unavailable to use for about a week. The deputy chairperson of the AU Commission said they had experienced

a 'massive cyber-attack'.[63] On top of this, in March 2024, failure in the under-ocean internet fibre optic cables infrastructure disrupted internet connection to governments, organisations, companies and people from South Africa, Nigeria, Ivory Coast, Liberia, Benin, Ghana, Burkina Faso and other countries.[64] African Union member states and the AU commission changed tactics: pivoting to publicly sharing information on malicious incidents and even mandating the development of a common African position on the applicability of international law in cyberspace to further African perspectives.

This shift is often described as taking place because of increased awareness of ICT security challenges, which have been thoroughly discussed in the OEWG 2021–2025 and supported by capacity building and increased engagement on ICT security from strategic partners such as the European Union (EU), yet with varying strategic priorities. Capacity building for African states was meant to increase the number of states participating in negotiations to ensure the OEWG 2021–2025 is more diverse than the previous session, and to facilitate the implementation of UNGGE and OEWG consensus recommendations. African diplomats and their counterparts have worked to move these issues forward.

---

[63] *Undersea Cable Damage Causes Internet Outages Across Africa*. (2024, March 14). https://www.dailymaverick.co.za/article/2024-03-14-undersea-cable-damage-causes-internet-outages-across-africa/

[64] *African Union's systems crashed by 'Massive' cyber attack, report says*. (2023, March 15). The Pan Afrikanist. https://thepanafrikanist.com/african-unions-systems-crashed-by-massive-cyber-attack-report-says/

In practice, however, this shift was already in motion before the OEWG 2019–2021. Though their rhetoric was different, in both processes, states paired African perspectives with strategic engagement in their approach to international ICT security. The parallels between OEWG and GGE positions suggest that African member states are unlikely to change their perspectives. In the UNGGE, the African member states' positions involved insisting on safeguards to avoid wrongful attribution of malicious incidents and the importance of balancing strategic security with peaceful use of cyberspace for development and economic prosperity. Insisting on these positions was projected to cause other GGE experts to consider the cost of public attribution by developing countries, more than likely to developed counterparts.

In 2018, cylinders containing toxic chlorine gas were dropped in a civilian-inhabited area in Douma, killing 43 and affecting dozens more. Considered a neutral investigator, the Organisation for the Prohibition of Chemical Weapons (OPCW)'s technical secretariat was given a mandate to identify the perpetrators of chemical weapons use.[65] Reflecting on this incident and parallels in the complexity of technical attribution, African experts proposed an independent mechanism to review claims and evidence, and sought to encourage clarity and confidence in the attribution process to spark a conversation about accountability in international ICT security discussions.

[65] *OPCW releases third report by investigation and identification Team*. (2023, January 27). OPCW. https://www.opcw.org/media-centre/news/2023/01/opcw-releases-third-report-investigation-and-identification-team

This proposal would later be somewhat inferred in the UN Secretary-General's policy brief calling for an 'independent multilateral accountability mechanism for malicious use of cyberspace by States to reduce incentives for such conduct and enhance compliance with agreed norms and principles of responsible State behaviour'.[66]

But African experts also showed a pragmatic side. They laid out a path to advance peaceful use of cyberspace, and cyberspace for economic development and prosperity, to balance the political and military use of cyberspace. The path was hamstrung by the narrow mandate of the First Committee, focused on peace and security and not issues of digital connectivity, but it nevertheless emphasised benefits of implementing norms to prevent conflict rather than downsides—evidence of Africa's approach to emerging security issues. The path also called for capacity building and emphasised a proposal for investment in human resources and educational programmes.

This African pragmatism was spearheaded by experts from South Africa and Kenya, who combined institutional memory of previous UNGGEs and careers in multilateral peace and security. With the other two experts, it may have seemed not to produce results, but they certainly demonstrated Africa's interest and capacity to engage and challenge existing

[66] United Nations. (2023). *Our Common Agenda Policy Brief 9: A New Agenda for Peace*. https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-new-agenda-for-peace-en.pdf

paradigms even as war-and-peace rhetoric dominated the negotiations.

This pragmatism was echoed in 2021, when the OEWG consensus report reflected and lifted UNGGE text. By this point, the UNGGE had concluded its work and the report considered a milestone.[67] That both OEWG and GGE experts from African states sought to advance independent mechanisms and due diligence in the attribution process and a primary priority to use cyberspace for development means that they all recognised the constraints of African states in terms of operating in the international ICT security environment with comparable technical and strategic advantage.

Years of international ICT security as a first committee agenda item failed to capture the attention of African states. The first committee mentions were buried between other agenda items on disarmament and non-proliferation, pushing ICT security to the periphery even as an emerging global security concern. Then came the expansion of UNGGE country experts from one African country in 2009–2010 (South Africa) and 2012–2013 (Egypt) to three in 2014–2015 (Kenya, Ghana and Egypt) and four in 2019–2021. The increase in representation contributed to an increase in national discussions to support experts. Repeated country representation succeeded in developing institutional memory transferable to African counterparts.

---

[67] CyberPeace Institute. (2021, June 9). *The UN GGE Final Report: A milestone in cyber diplomacy, but where is the accountability?* https://cyberpeaceinstitute.org/news/the-un-gge-final-report-a-milestone-in-cyber-diplomacy-but-where-is-the-accountability/

Strategic partner competition is also shaping Africa's approach towards international ICT security. Bilateral and inter-regional cooperation such as an Africa–Russia Summit and EU–AU cooperation have created opportunities for African states to deepen their influence in multilateral discussions such as the OEWG. Since negotiation of the OEWG 2021–2025 mandate in 2021—which prompted the resolution sponsors and opposers to substantially engage African states on the modalities and substantive text or risk failure—there has been a growing recognition that it is not in the interests of any bloc or region to engage African counterparts and leaders marginally. Since Africa is the fastest growing continent, in population and strategic power, as seen for example in the recent admission of the AU to the G20, it will continue to be important for multilateral governance and strategic partners.

Reflecting on Africa's approach is a reminder for African emerging leaders in international ICT security—diplomats and policymakers—that starting from scratch is not necessary. The good practices and toolbox for effective diplomacy are well defined. Emerging leaders now have AU structured processes such as the AU cybersecurity expert group for developing and reviewing positions, including on the nexus between ICT security and issues of emerging technologies and the Sustainable Development Goals. The AU Commission on International Law's facilitation of the Common African Position on the applicability of international law (CAP-IL), including international humanitarian law, provided a well-defined process for the consultation and training of national officials and diplomats in Addis Ababa, New York and Geneva. Any emerging leaders that want to engage effectively in the OEWG

and future intergovernmental forums can leverage these initiatives.

African states should be encouraged to continue to engage in international ICT negotiations in and outside the UN forum—even with states and regions with which they have previously not been likeminded. In the past, engaging with traditional partners led to an easier path to consensus. Unless accompanied by new forms of engagement and negotiation, traditional partners alone will not lead to the level of impact and influence that African states can effect.

Moliehi Makumane

Security and Technology Programme Researcher, UNIDIR

Moliehi Makumane is a researcher with the Security and Technology Programme at UNIDIR. Her expertise spans the international cybersecurity domain with emphasis on the implications of emerging technologies for security in developing countries. Before joining UNIDIR, Moliehi was with South Africa's Department of International Relations and Cooperation where she led the international cybersecurity file, as negotiator in the OEWG and a senior advisor in the UN GGE. She also worked on the Inter governmental expert Group on cybercrime. She holds an Honours Degree in political and international studies from Rhodes University, Makhanda, South Africa. She speaks English and South Sotho. Moliehi's areas of expertise include international ICT security and international cybercrime.

Regional Organisations and Confidence-Building Measures

Szilvia Tóth

Confidence-building measures (CBMs) are one of the pillars of the International Framework of Responsible State Behaviour in Cyberspace. While the relevant UN reports contain recommendations for CBMs on a global level, regional organisations have been the main drivers of efforts on developing and implementing regional cyber CBMs. The first regional organisation to do so was the Organization for Security and Co-operation in Europe (OSCE); the Association of Southeast Asian Nations (ASEAN) and the Organization of American States (OAS) followed this example half a decade later. Ten years after the adoption of the first set of OSCE cyber CBMs, the measures remain relevant and impactful. How did a traditional mechanism on arms control become a practical instrument for regional cooperation on cyber issues and a tool for enhancing national cyber resilience?

Developing OSCE's cyber/ICT security CBMs

OSCE's work on cyber issues has always been connected to and determined by the UN processes on international ICT security. While the UN GGE report of 2010 formulated recommendations for CBMs, for most states cyber issues were a topic for technical experts, but nothing diplomats should engage with. However, for the United States—which initiated the proposals on CBMs in the UN—the OSCE seemed well placed to start discussions on cyber CBMs. With its vast history and experience on traditional arms control, the concept of confidence- and security-building measures was familiar to diplomats in Vienna. Thus, the OSCE participating states decided to set up a working group to develop and negotiate regional cyber/ICT security.

Work began immediately and in parallel to the 2012–13 UN GGE. These efforts resulted in the adoption of 'The initial set of OSCE Confidence-building Measures to reduce the risks of conflict stemming from the use of information and communication technologies'[68] at the end of 2013. After this first success, states continued discussions and negotiations on a second set of CBMs—again in parallel to the 2014–15 UN GGE process—adding five additional cooperative measures to the initial set.[69] In a span of just four years, OSCE participating states have agreed on 16 CBMs, to which—although they are non-binding and voluntary—states have made a political

[68] https://www.osce.org/files/f/documents/d/1/109168.pdf
[69] https://www.osce.org/files/f/documents/d/a/227281.pdf

commitment to adhere. The aim of CBMs is to enhance interstate cooperation, transparency, predictability and stability, as well as to reduce the risks of misperception, escalation and conflict that may stem from state use of ICTs.

The years between 2012 and early 2016 proved to be a time of constructive engagement by OSCE participating states, with a focus on negotiating the text of the CBMs. While this is a huge achievement, it also needs to be emphasised that the actual text of the measures is the result of finding balance between often competing national positions, to be able to reach consensus. For CBMs to be meaningful, they need to be implemented.

Multilateral processes benefit from states—and, even more importantly, committed individuals—moving issues forward and bringing in innovative ideas. This was the case within the OSCE as well. With the aim of moving forward the practical implementation of the CBMs, to endow the consensus text with meaning, a few states, actively engaged in the OSCE cyber process, took the lead—through their cyber diplomats—in proposing concrete ideas for the operationalisation of the CBMs, for example detailing a process for consultations (CBM No. 3) or laying down the foundations for an operational cyber Point of Contact Network (CBM No. 8).

Shifting the focus to CBM implementation

After 2017, the geopolitical situation deteriorated and the failure of the 2016/17 GGE significantly affected the

atmosphere within the OSCE, resulting in a shift from consensus-based negotiations to increased efforts put into the practical implementation of the CBMs. The working group on cyber issues became a platform to share information on national implementation of CBMs; furthermore, states volunteered to champion efforts on OSCE-wide operationalisation of the CBMs. The latter became the 'Adopt-a-CBM' initiative, where individual states or a group of states explore concrete modalities for achieving CBM implementation. By the end of 2023, nine CBMs had been adopted by 23 participating states.

Concrete outcomes of the work of the 'CBM adopters' include, for example, an e-learning course on coordinated vulnerability disclosure[70] (CBM No. 16) and how to set up national policies to facilitate this process; a report compiling recommendations for setting up national cyber-incident classification systems (CBM No. 15),[71] based on the OSCE experience; a report sharing good practices in setting up public–private partnerships for cybersecurity (CBM No. 14);[72] and a glossary of cybersecurity-related terminology collected from official documents of the OSCE participating states (CBM No. 9).[73]

It was equally important to ensure that all OSCE participating states benefit from the CBM process. Implementing CBMs inherently builds capacities. With the intention to raise

[70] https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCVD+2022_04/about
[71] https://www.osce.org/files/f/documents/6/5/530293_1.pdf
[72] https://www.osce.org/files/f/documents/2/7/539108_0.pdf
[73] https://cbm9.gov.rs/

awareness on the CBMs, trainings were organised to familiarise states with the concept, offer expert advice and also practise the applicability of the measures. Such events not only helped build confidence and trust between states, but also started to build partnerships in a subregional setting. The main objective of CBMs is to avoid the risk of conflict and escalation, therefore if neighbours know each other and have previously engaged with each other, these risks are significantly reduced. Through the knowledge sharing happening during these events, national cyber capacities are built as well.

One of the flagship initiatives of the OSCE is its cyber Point of Contact Network (CBM No. 8), a database of contact details of policy and technical focal points, who can reach out to each other in case of an incident or to request specific information. The database is kept up to date as much as possible, through regular communication and information sharing. Almost all participating states have provided these details. One might think that since it is about cyberspace, having email addresses of counterparts is enough to build confidence and trust. This is not the case at all. Putting a face to the name having met in person is the way to ensure cooperation and partnerships and build a community of policymakers and technical experts. The annual meeting of the OSCE cyber Points of Contact is a testament to this.

Can CBMs developed for peacetime remain relevant in times of conflict?

CBMs have been developed in the context of international peace and security with the intention to avoid the risk of conflict. When Russia launched its war of aggression against Ukraine in February 2022, the question arose as to whether the CBM process could remain relevant in the OSCE while two of the participating states were engaged in an armed conflict.

With the experience accumulated in implementing CBMs, their purpose grew beyond their initial purpose of avoiding risk of conflict or escalation. The meaningful implementation of CBMs has become an instrument of cooperation and knowledge sharing, which build capacities and enhance national cyber resilience. These are valuable characteristic in times of increasing conflict and geopolitical tensions. Not only have participating states remained engaged in the cyber discussions at the OSCE, but the number of states contributing to the process is continuously rising, attesting to the value of CBM implementation and its relevance in ensuring international cooperation in cyberspace.[74]

The results achieved on practical implementation of CBMs at regional level also inform the discussions at UN level at the 2nd OEWG, and will remain relevant for any future mechanism dealing with international cyber policy.

[74] *10 years of OSCE Cyber/ICT Security Confidence-Building Measures*. (2023, October 24). OSCE. https://www.osce.org/secretariat/555999

Szilvia Tóth

Cyber Security Officer at the Secretariat of the Organization for Security and Co-operation in Europe (OSCE).

Szilvia Tóth currently works as the Cyber Security Officer at the Secretariat of the Organization for Security and Co-operation in Europe (OSCE). In her scope of work she is responsible for supporting participating States in cyber related matters, including assistance in developing and implementing cyber Confidence Building Measures. Previously Ms. Tóth was a diplomat at the Ministry of Foreign Affairs of Hungary, working on cyber diplomacy issues and EU affairs. Before joining the Ministry of Foreign Affairs, she worked in the private sector: at the mobile phone operator Vodafone Hungary and fixed-line telecom service provider United Telecom Investment. She holds a Bachelor's degree in International communications and a Master's degree in European Union affairs.

The views expressed in this essay are solely those of the author and do not necessarily reflect the views and mandate of the Organization for Security and Co-operation in Europe (OSCE).

Cybersecurity and Its Influence on Traditional Diplomacy in the Americas

Kerry-Ann Barrett

The Americas is a region characterised by great diversity in technological development, cyber-threat preparedness and resiliency. Today we can see varying perceptions of risk and vulnerability, varying degrees of implementation of international standards and instruments, and varying levels of prevention and response capacities. This diversity is also reflected in varying degrees of cooperation, at all levels—national, bilateral, regional, and international—and among all relevant stakeholders. More specifically, it is in this regard that we see cybersecurity shifting the well-established art of diplomacy to be more inclusive, and now not just involve nations but also take account of the role of individuals, technology actors and other non-state actors at the table.

This multistakeholder collaborative approach to addressing cyber threats recognises that no single organisation, state or region can succeed in preventing and countering threats to cyberspace in isolation. The stability of a state directly—and indirectly—affects the stability not just of its neighbours but also of those it has ties with. Latin American and Caribbean countries over the years have emphasised the importance of Information and Communication Technology (ICT) in

promoting economic growth, social development and connectivity in the region. The need for investment in capacity building in order to meaningfully participate in decision-making processes within the framework of the United Nations (UN) has been highlighted as critical as well. Without a doubt, countries in the region have called for increased cooperation and collaboration on cybersecurity and digital innovation to harness the potential of ICT for sustainable development.

However, this cannot be considered in a vacuum. With the focus on responsible state behaviour in cyberspace, the discussions over the various Groups of Government Experts (GGEs), Open Ended Working Groups (OEWGs) and the Ad Hoc Committee on cybercrime have provided a platform for states to discuss and potentially develop norms and frameworks on cybersecurity and cybercrime. With each process, what has been interesting to observe is the emergence of the role of smaller developing nations as lead coordinators for negotiations, in fora where traditionally they have called for more capacities.

Several factors could have impacted this: on one hand, the increased availability of cyber-diplomacy courses through the OAS/CICTE Cybersecurity Program and other partners and on the other hand, increased funding opportunities to fellows[75] and other travel support offered to the developing regions,

[75] EU Cyber Direct. (n.d.). *Good Cyber Story: Women and International Security in Cyberspace Fellowship*. Horizon. https://eucyberdirect.eu/good-cyber-story/women-and-international-security-in-cyberspace-fellowship

including Latin America and the Caribbean, to participate in negotiating processes, where in the past travel cost would have been prohibitive.

This increased participation has increased in tandem with individual Latin American and Caribbean countries developing their own cyber-diplomacy strategies as well. Some countries such as Brazil and Costa Rica have articulated their position on the applicability of international law to cyberspace, while others are more active in shaping global norms in cyberspace and including this concept as part of their national cybersecurity strategies. For example, Brazil in its national statement stated that:

> Brazil firmly believes that in their use of information and communications technologies, States must comply with international law, including the United Nations Charter, international human rights law and international humanitarian law … Brazil firmly believes that in their use of information and communications technologies, States must comply with international law, including the United Nations Charter, international human rights law and international humanitarian law.[76]

This state of play on this is ongoing as many countries in Latin America and the Caribbean are become larger consumers of

[76] United Nations. (2021a). *Developments in the field of information and telecommunications in the context of international security*. https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

technology, which by extension makes cybersecurity an essential part of foreign and security policies.[77]

The developing nation lens

Many Latin American and Caribbean countries lack the resources to invest in cybersecurity infrastructure and expertise as compared to their more developed nation counterparts in this space. Given the various national realities, countries therefore have varying levels of cyber threats and priorities, making regional cooperation a challenge.

However, Latin American and Caribbean countries do offer a unique perspective on cyber diplomacy, as they have continued to emphasise:

- Peaceful uses of technology: Recognising the benefits of cyberspace for development and cooperation
- Multistakeholder approach: Involving civil society, the private sector and academia in cyber policy discussions.

This perspective has brought the discussion at the UN level to focus on a stable, secure and inclusive digital space. Human rights online, particularly freedom of expression and privacy and balancing security needs with these rights, remains a key focal discussion point, as evidenced in the various interventions in both the recent OEWG and Ad Hoc Committee processes.

[77] *Cyber Policy Portal*. (n.d.). https://cyberpolicyportal.org/

Institutional regional and institutional contribution

By extension, at the Organization of American States (OAS), several efforts to facilitate cyber diplomacy have been centred around cyber capacity building aimed to promote regional cooperation. Regional organisations such as the OAS have long acted as interlocutors for implementing UN mandates at the regional level by helping member states to have the capacity to fulfil their various international obligations. OAS, too, was one of the first to discuss the issue of cybersecurity both regionally and globally, adopting resolutions and recommendations since 1999. Our member states have been able to meet, discuss and reach consensus on the subject of cybersecurity without the need for a new treaty. This is particularly true for cybersecurity capacity building, where the OAS has been working specifically on the topic of cybersecurity for nearly 20 years with various partners including UN agencies and bodies, to help ensure that international responses take into account the cybersecurity challenges and related social, economic and security considerations faced by our hemisphere.

OAS member states agreed recently to establish a Working Group on Cooperation and Confidence Building Measures in Cyberspace.[78] This Working Group was approved by OAS

[78] Eleven agreed CBMs in cyberspace:

1. Provide information on national cybersecurity policies, such as national strategies, white papers, legal frameworks and other documents that each member state considers relevant.
2. Identify a national point of contact at the political level to discuss the implications of hemispheric cyber threats.
3. Designate points of contact, if they do not currently exist, in the Ministries of Foreign Affairs with the purpose of facilitating work for cooperation and international dialogues on cybersecurity and cyberspace.
4. Develop and strengthen capacity building through activities such as seminars, conferences, and workshops, for public and private officials in cyber diplomacy, among others.
5. Encourage the incorporation of cybersecurity and cyberspace issues in basic training courses and training for diplomats and officials at the Ministries of Foreign Affairs and other government agencies.
6. Foster cooperation and exchange of best practices in cyber diplomacy, cybersecurity and cyberspace, through the establishment of working groups, other dialogue mechanisms and the signing of agreements between and among States.
7. Encourage and promote the inclusion, leadership, and effective and meaningful participation of women in decision-making processes linked to information and communication technologies by promoting specific actions at the national and international levels, with the aim of addressing dimensions around gender equality, and the reduction of the gender digital divide, in line with the women, peace, and security agenda.
8. Promote study, discussion, development, and capacity-building at the national and international levels regarding the application of international law to the use of information and

member states in 2017 through resolution CICTE/RES.1/17, given the need for increased cooperation, transparency, predictability and stability among states in the use of cyberspace. The group focuses on non-traditional confidence-building measures (CBMs), specifically those related to cyberspace.

The CBMs themselves allude to the need to build capacities, and as such several of our member states, in addition to the support needed in building their capacities in diplomacy and international law in cyberspace, require basic support such as in the construction of a national resilient cybersecurity framework, which is consistent with the emerging new threats. In recognition of the need for a legislative framework, the OAS Cyber Crime Working Group of Ministers of Justice and

---

communications technologies in the context of international security by promoting voluntary exchanges of positions and national vision statements, opinions, legislation, policies, and practices on the subject, in order to promote common understandings.

9. Promote the implementation of the 11 voluntary, non-binding norms on responsible State behavior in cyberspace adopted by resolution 70/237 of the General Assembly of the United Nations and promote reporting on these efforts taking into account the national implementation survey.
10. In the sphere of information and communication technologies, promote work and dialogue with all stakeholders, including civil society, academia, the private sector, and the technical community, among others.
11. Develop national cyber incident severity schemas and share information about them.

Prosecutors of the Americas, within the framework of REMJA,[79] offers capacity development workshops to help member states develop instruments laws to investigate and prosecute cybercrimes better, a large part of which is transnational in nature.

Cybersecurity coordination and cooperation have proved to be pivotal elements in the pursuit of mitigating the risks of conflict in cyberspace. Undoubtedly, inter-regional cooperation and collaboration presents an opportunity at a minimum for dialogue, as this will enable the possibility to create synergies and build upon consensus around common topics to define concrete actions. To this extent, the OAS has focused on expanding its cooperation agreements with different stakeholders, as well as serving a unique role as a platform of engagement to achieve a broader global agenda in its role as the Global Forum of Cyber Expertise (GFCE) Hub for the Americas, while contributing to the applicability, implementation, commitment and monitoring of UN processes.

Final reflection

The reality is, diplomats and other government officials from throughout the region require a greater understanding of cyberspace-related concepts and issues to engage, participate and negotiate meaningfully in international fora. The OAS has been implementing three different types of cyber-diplomacy

[79] The Organization of American States (OAS). (n.d.). *Cooperation in Justice-REMJA*. https://www.oas.org/en/sla/dlc/remja-en/remja.asp

programmes that cover internet governance and the work of the first and third committee as it relates to cybersecurity and cybercrime, and have been facilitating and will continue to facilitate these courses for our member states. Further, as many countries emerge from the aftermath of the COVID-19 pandemic, administrative changes with the most recent presidential elections, aligning foreign investment with development agendas, are key. Latin America and the Caribbean are therefore by necessity strengthening multilateral international cooperation: this includes how they manage cyber-diplomatic encounters. Dialogues that foster collaboration between regions are essential to enhance global cybersecurity and contribute to a free, open, safe and secure cyberspace, in view of the new challenges posed by emerging technologies.[80]

[80] One of the more specific initiatives is the Europe and Latin America and the Caribbean (LAC) Digital Alliance. International cooperation between LAC and the EU allows for the exchange of experience and best practice, and this multistakeholder cooperation enhances regional and global cybersecurity resilience: EEAS. (2024, February 16). *Europe and Latin America & the Caribbean step up cooperation on cybersecurity*. https://www.eeas.europa.eu/eeas/europe-and-latin-america-caribbean-step-cooperation-cybersecurity_en?s=160

Kerry-Ann Barrett

Section Chief of the Cybersecurity Section within the Inter-American Committee Against Terrorism of the Organization of American States (OAS/CICTE)

Kerry-Ann Barrett, is the Section Chief of the Cybersecurity Section within the Inter-American Committee Against Terrorism of the Organization of American States (OAS/CICTE) and coordinates the cybersecurity capacity building efforts to OAS member states. She is a trained attorney at law with over 20 years of public sector and multi-lateral experience, and leads a team of professionals to deliver strategic cybersecurity capacity intervention. Through the design, planning and execution of cybersecurity initiatives, including: development and implementation of National Cybersecurity Strategies; provision of Technical Training to policy makers and technical public officers, establishment and strengthening of national cybersecurity incident response teams (nCSIRTs) and facilitation of cybersecurity awareness tools, she currently supports countries in Latin America and the Caribbean. Additionally, she is an expert public speaker on regional and international cyberspace topics, with a focus on cyber-related issues in Latin America and the Caribbean. Kerry-Ann has extensive public sector and multi-lateral experience in cybersecurity policy development, internet governance and cybersecurity risk mitigation. She possesses a Post Graduate Diploma in International Arbitration, a Master's in Business Administration (Distinction) in International Business, a Bachelor of Law (LLB. with distinction) and Certificates in E-Diplomacy, Cyber Security Risk Management and Legal Frameworks for ICTs. Mrs. Barrett holds several

designations such as a member of the Board of Curators for the portal on cybersecurity capabilities of the University of Oxford, an Oxford Martin Associate as a member of the Global Cyber Security Capacity Centre's Expert Advisory Panel, a member of the Advisory Group focusing on the principles of Cyber Capacity Building under Chatham House and the Advisory Committee of the Humanitarian Cybersecurity Centre under the Cyber Peace Institute.

From Deterrence to Initiative Persistence in Cyberspace: NATO's Changing Role in Cyber Diplomacy

Ben Hiller

As the world's largest military alliance, NATO plays a unique role in global cyber diplomacy. What NATO says and does impacts on international cyber stability.

NATO's announcement in 2014 that a cyberattack can lead to the invocation of Article 5—the Alliance's collective defence clause[81]—and the decision in 2016 to designate cyberspace as a domain for operations[82] fed unfounded Russian and Chinese narratives of the 'West' militarising cyberspace.[83]

Today, NATO Allies battle an avalanche of disinformation from Russia, including fake news and hybrid campaigns that have

---

[81] NATO. (2014, September 5). *Wales Summit Declaration*, para 72, [Press release]. https://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber

[82] NATO. (2016, July 9). *Warsaw Summit Communiqué* [Press release]. https://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber

[83] Stevens, T., and Burton, J. (2023, June 6), *NATO and Strategic Competition in Cyberspace*, *NATO Review*, https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html

increased markedly since Russia's full-fledged invasion of Ukraine.

Russian disinformation, including on cyber, has gained a lot of traction in the 'Global South', and Allies were (and are) often confronted with this narrative at UN and regional cyber-stability discussions and negotiations: for instance, in discussions on the applicability of international law in cyberspace and the right to self-defence.

A complicating factor for pushing back against this false description of the Alliance's approach to cyberspace was differing views across the Alliance as to how much NATO as an organisation should get involved in cyber-diplomacy efforts. In fact, until recently many cyber diplomats believed NATO should stay well away from discussions at the UN and elsewhere 'because it may complicate consensus building'.

Russia's war of aggression against Ukraine—including in cyberspace—has further sharpened Allied cyber diplomacy. Allies are actively reasserting NATO's approach and contribution to international cyber stability. Such positioning starts with the simple fact that NATO's cyber-defence approach is and has always been defensive, and responsive to an ever-evolving threat landscape.

In fact, NATO only issued its first cyber defence policy after the cyberattacks on Estonia in 2007 and the use of malicious cyber

capabilities during the conflict between Russia and Georgia in 2008.[84]

At the core of all NATO cyber-defence activities is the full respect of international law, including the UN Charter, international humanitarian law and international human rights law. NATO promotes a free, open, peaceful and secure cyberspace.[85]

Allies have reiterated on several occasions that they expect all UN member states to live up to their commitment to behave responsibly in cyberspace.[86] Those who do not respect the rules or who act irresponsibly should rightfully expect consequences.

They clarified[87] that they are prepared to make use of the full range of capabilities to deter, defend against and counter the full spectrum of cyber threats; and to use NATO as a platform to enhance national cyber resilience and to impose costs, if

---

[84] NATO. (2024, July 30). *Cyber Defence*. https://www.nato.int/cps/en/natohq/topics_78170.htm

[85] NATO. (2021b, June 14). *Brussels Summit Communique*, para 66 [Press release]. https://www.nato.int/cps/cz/natohq/news_185000.htm

[86] As evident in recent statements by the North Atlantic Council. See e.g. 'Statement by the North Atlantic Council concerning the malicious cyber activities against Albania' (2022), https://www.nato.int/cps/en/natohq/official_texts_207156.htm; or 'Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise' (2021), https://www.nato.int/cps/en/natohq/news_185863.htm

[87] NATO. (2021b, June 14). *Brussels Summit Communique*, para 66 [Press release]. https://www.nato.int/cps/cz/natohq/news_185000.htm

necessary, collectively. Responses can draw on the entire NATO toolbox including political, diplomatic and military tools. Cyberattacks are not necessarily to be met with cyber responses.[88]

In this context, it is important to emphasise that NATO is not the only multilateral platform at Allied disposal to implement a norms-based approach to cyberspace. An intriguing detail is that until today some Allies see different platforms as coming into play at different points in time. This decision is largely driven by escalation management considerations.

At one end of the spectrum are mechanisms such as the OSCE's cyber confidence-building measures (CBMs)[89] as a way to avoid potential friction and/or escalation; in the middle the EU Cyber Diplomacy Toolbox;[90] and at the other end NATO—a platform perceived by many as synonymous with 'hard power'.

However, the perception of NATO at the end of the escalation ladder, or as a last resort for imposing costs, is shifting with a change in how the Alliance perceives cyberspace. Following Russia's full-scale invasion of Ukraine, Allies are set to further refine NATO's toolbox to address malicious cyber actors.

---

[88] NATO. (2021b, June 14). *Brussels Summit Communique*, para 66 [Press release].
https://www.nato.int/cps/cz/natohq/news_185000.htm
[89] See OSCE. (n.d.). *Cyber/ICT Security*.
https://www.osce.org/secretariat/cyber-ict-security
[90] See EU Cyber Diplomacy Toolbox. Cyber Risk GmbH. (n.d.). *The EU Cyber Diplomacy Toolbox: An In-Depth Analysis of Cyber Diplomacy*.
https://www.cyber-diplomacy-toolbox.com/

At the 2023 NATO Summit in Vilnius, Allies endorsed a new Concept[91] to enhance the contribution of cyber defence to NATO's overall deterrence and defence posture. Central to the Concept is a shared understanding that cyberspace is contested at all times, and never at peace. There are continuous cycles of escalation and de-escalation in cyberspace requiring a 'campaign-style' mindset.[92]

This is why in Vilnius Allies reiterated that the cumulative effects of a campaign of malicious cyber activities can equally trigger Article 5 under certain circumstances. In other words, adversaries and strategic competitors should not feel too comfortable that the Alliance will be idle as they continuously test the limits in the 'grey' space below Article 5.

Allies also decided to further integrate NATO's three cyber-defence levels—political, military and technical—and ensure civil–military cooperation at all times, through peacetime, crisis and conflict. This led to the decision at the 2024 Washington Summit to set up a NATO Integrated Cyber Defense Centre (NICC), co-locating NATO stakeholders, Allies and industry on a 24/7 basis.[93]

---

[91] NATO. (2021b, June 14). *Brussels Summit Communique*, para 66 [Press release]. https://www.nato.int/cps/cz/natohq/news_185000.htm

[92] Van Weel, D. (2023). *A Proactive Approach to the Cyber Domain Strengthens NATO's Deterrence and Defense Posture*. Digital Front Lines. https://digitalfrontlines.io/2023/07/13/proactive-approach-to-the-cyber-domain/

[93] NATO. (2024a, July 10). *Washington Summit Declaration*, para 7 [Press release]. https://www.nato.int/cps/en/natohq/official_texts_227678.htm

There are two underlying reasons for this: first, to avoid 'magic handovers' between civilian and military cyber stakeholders as cyber crises intensify or decrease; and second, to synchronise in one place political, military and technical cyber efforts to continuously increase the costs and reduce the benefits for malicious threat actors.

The Concept moves the Alliance away from the 'response-follows-attack' logic applicable in kinetic warfare, towards the recognition that this approach has limited applicability in a continuously contested environment such as cyberspace.

Another way Allies are bolstering NATO's capacity to deal with malicious cyber activities below the threshold is new strategic measures endorsed at the Washington Summit in 2024 to address significant malicious cyber activities and campaigns—NATO's very own cyber-diplomacy toolbox.

The measures further broaden NATO's ability to support the full application of international law in cyberspace as well as observance of norms of responsible state behaviour during peacetime.

Among other enablers, the strategic measures will reform how NATO's Cyber Defence Committee[94] does business. There is a shift from a reactive to a proactive policy approach. This approach will better track malicious cyber actors across the

[94] The Cyber Defence Committee, subordinate to the North Atlantic Council, is NATO's lead committee for political governance and cyber-defence policy.

Alliance, allow Allies to connect the dots, and continuously update potential responses to specific threat actors.

The Concept and the strategic measures signal NATO's preparedness to play a more active role in international cyber diplomacy. Both are responses to Russia's war of aggression on Ukraine, and China continuing to erode fundamental freedoms online.

Whether NATO will become more visible in international cyber diplomacy remains to be seen. It will be up to each and every Ally to determine how they engage NATO as a platform to manage an increasingly turbulent cyber-threat landscape as part of strategic competition.

Ben Hiller

Senior Policy Officer for Cyber and Hybrid issues, NATO

Ben Hiller is a Senior Policy Officer for Cyber and Hybrid issues at NATO. In his role, he developed the Alliance's current Cyber Defence Policy, the framework for NATO's Integrated Cyber Defense Centre, and most recently NATO's strategic measures to address malicious cyber campaigns below the Article 5 threshold. Before joining NATO, Ben was responsible for cyber policy at the Organization for Security and Co-operation in Europe (OSCE). In his role he guided efforts in developing and operationalizing confidence building measures (CBMs) to reduce the risks of conflicts stemming from the use of cyber capabilities between States. Before that, Ben worked on counter terrorism issues, focusing on the use of technology and biometrics for the secure

cross-border movement of people and goods across Europe, the Caucasus and Central Asia.

Disclaimer: The views of the author may not reflect the views of the Alliance.

Strengthening Cyber Diplomacy: The ASEAN Experience

Sithuraj Ponraj

Cyber diplomacy is a multidisciplinary team effort

Like cybersecurity, cyber diplomacy is itself a team effort. While diplomats often lead in international cyber discussions, skilfully navigating diplomatic processes and language, they are being increasingly supported by cyber policy, operational and legal subject matter experts who are familiar with the technical aspects of the cyber domain. Given the cross-cutting nature of cybersecurity, successfully negotiating international and regional cyber discussions often requires careful coordination between such multidisciplinary teams.

The Association of Southeast Asian Nations (ASEAN) as a bloc is a relative newcomer to international cyber diplomacy. A regional grouping comprising 10 member states with diverse political, economic, historical, social, cultural and linguistic backgrounds[95] and at different stages of their digital and cyber

[95] ASEAN membership comprises Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore,

developmental journeys, its aim is to promote political security and economic and social cooperation among countries in the region, as well as cooperation and dialogue with countries in the wider international community.

At the same time, ASEAN has since its inception been strongly united in its support for an inclusive international rules-based multilateral order where the voices of all states—both large and small—are equally heard within the community of nations, and based on mutual respect, non-interference, settlement of disputes in a peaceful manner, renunciation of the threat or use of force, and effective cooperation—all of which are themselves fundamental ASEAN principles.[96] ASEAN member states have actively espoused these perspectives during their increasingly active participation in international cyber discussions, including those at the UN.

ASEAN's emphasis on a rules-based multilateral order, inclusiveness and strong cooperation—all of which can foster stability, trust and confidence in the international system—is backed by an economic, as well as a national security, imperative. As a young, dynamic region with a digital economy that is poised to grow from $300 million to $1 trillion by 2030, and a population of close to 700 million made up of a significant proportion of young, educated, online-savvy

---

Thailand and Vietnam. In November 2022, ASEAN member states agreed 'to grant Timor-Leste an observer status and allow its participation in all ASEAN Meetings' [para 2, ASEAN Leaders' Statement on the Application of Timor-Leste for ASEAN Membership].

[96] These fundamental principles are contained in the Treaty of Amity and Cooperation in Southeast Asia, established in 1976.

individuals and a growing middle class,[97] ASEAN member states without distinction see the adoption of digital technologies as an opportunity to ensure economic progress, accelerate development, achieve Sustainable Development Goals and ensure better living standards for their people.

In this regard, ASEAN member states have long recognised the vital importance of cybersecurity as a key enabler in ensuring the safe, secure and trusted use of these technologies. As such, the building of strong national cyber capabilities to ensure cyber resilience against cyber threats and attacks and the establishment of a secure, safe, trusted, open and interoperable cyberspace undergirded by trust and confidence in a rules-based multilateral order have long been central to ASEAN's vision of the digital future.

Recognising the vital role that cyber diplomacy can play in advancing the establishment of an inclusive, rules-based, secure, open and interoperable cyberspace, ASEAN member states have undertaken several key regional efforts to build and support the capabilities of their interdisciplinary teams participating in international cyber discussions.

The efforts undertaken by ASEAN in recent years include (a) the strengthening of regional cybersecurity mechanisms to better support ASEAN member states in their own development of national cyber strategies, policies and diplomatic positions; (b)

---

[97] Lee, J. O. (2024, January 12). *Young people in ASEAN are embracing digitalization*. https://www.weforum.org/stories/2024/01/asean-building-trust-digital-economy/

the deepening of cyber-policy exchanges with external partners; and (c) the advancing of coordinated regional cyber capacity-building programmes to build the capabilities of multidisciplinary teams at the national level.

Strengthening regional cyber mechanisms

The 2018 ASEAN Leaders' Statement on Cybersecurity Cooperation

The ASEAN Leaders' Statement on Cybersecurity Cooperation,[98] which was endorsed at the 32nd ASEAN Summit under Singapore's chairmanship in April 2018, has given a key impetus to ASEAN efforts in this direction. It has the distinction of being the first such statement by ASEAN leaders on the topic of cybersecurity, and it has continued to provide a strong mandate and starting point to guide the forward efforts to enhance regional cybersecurity architecture and cyber diplomacy. It underscored ASEAN's shared vision of a peaceful, secure and resilient cyberspace that served as an enabler of economic progress, enhanced regional connectivity and better living standards for all.

In addition to reaffirming the need to build closer cooperation and coordination among ASEAN member states and the value

[98] ASEAN. (2018a, April 27). *ASEAN Leaders' Statement on Cybersecurity Cooperation*. https://asean.org/asean-leaders-statement-on-cybersecurity-cooperation/

of enhanced dialogue and cooperation with Dialogue Partner countries and other external parties, the statement also highlighted the importance of continued efforts to strengthen the establishment of a rules-based international order in cyberspace. In particular, the statement recognised the need for all ASEAN member states to closely coordinate regional cybersecurity policy, diplomacy, technical and capacity-building efforts. It also tasked relevant ministers from all ASEAN member states to implement practical confidence-building measures (CBMs) and adopt a common set of voluntary, non-binding norms of responsible state behaviour in cyberspace, taking reference from norms set out in the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE).

Operationalising the ASEAN Leaders' Statement

With the statement as a foundational roadmap, ASEAN has continued to establish and strengthen coordination mechanisms to strengthen regional cybersecurity policy and operational and diplomatic cooperation. The ASEAN Digital Ministers' Meeting, or ADGMIN (formerly known as Telecommunications and Information Technology Ministers Meeting, or TELMIN), anchors the regional grouping's political commitment to exchanges and practical cooperation on issues related to the rapidly evolving digital landscape, including on

cybersecurity. Supported by senior officials meeting in the ASEAN Digital Senior Officials' Meeting (ADGSOM) and the ASEAN Network Security Action Council (ANSAC), ASEAN digital ministers have taken a forward-leaning stance in the development of five-year ASEAN Cyber Cooperation Strategies since 2015.[99] These ASEAN Cyber Cooperation Strategies serve to review the global and regional cyber-threat landscape, identifying current and emerging cyber threats of concern to the region and setting out strategic objectives for practical cooperation in areas such as information sharing, critical information infrastructure (CII) protection, capacity building and CBMs, as well as in the implementation of voluntary, non-binding norms of responsible state behaviour in cyberspace.

The location of regional cybersecurity discussions in a ministerial platform that sits in the ASEAN Economic Community pillar (unlike the cybercrime and defence-related cyber discussions that sit under the ASEAN Political-Security Community Pillar) has also allowed ASEAN digital ministers who oversee digital development in their respective countries to more easily identify and leverage synergies and cross-linkages between regional digital initiatives and cybersecurity efforts, ensuring that cybersecurity cooperation initiatives in

[99] The first ASEAN Cybersecurity Cooperation Strategy (2017–2020) was endorsed in 2017; the second Strategy (2021–2025) was endorsed in 2020. ASEAN member states are currently drafting a third Cybersecurity Cooperation Strategy that will set out the cybersecurity cooperation strategic objectives for the region from 2026–2030.

the region remained relevant to undergirding and advancing the region's economic and developmental goals.

At the same time, the security-related focus of the ASEAN Network Security Action Council (which reports to the ASEAN Digital Ministers' Meeting) has continued to ensure that the national security imperative is not lost but is balanced with the economic and developmental considerations in the ASEAN digital ministers' agenda. ASEAN digital ministers have continued to pay close attention to the need to address current and emerging cybersecurity threats and in recent years have endorsed multiple initiatives to improve regional cyber resilience. This includes the establishment of an ASEAN CERT Information Sharing Mechanism to facilitate timely information exchanges following the 2020 Solarwinds incident. Most recently, in February 2024, ASEAN digital ministers approved the establishment of an ASEAN Regional CERT. Located in Singapore, the ASEAN Regional CERT (to be launched in October 2024) will promote and facilitate timely information sharing and CERT-related capacity building among ASEAN member states and serve to complement the operational work of the existing national CERTs.

Responding to the leaders' guidance to closely coordinate regional cybersecurity policy, diplomacy, technical and capacity-building efforts, ASEAN has also established other structures and mechanisms to facilitate cross-cutting discussions among ASEAN ministers and senior officials overseeing various aspects of national cyber policy making.

The ASEAN Ministerial Conference on Cybersecurity (AMCC), held annually since 2016 on the sidelines of the Singapore

International Cyber Week, functions as a non-formal platform to discuss cross-cutting cyber policy, operational and diplomacy-related issues. The ASEAN Ministerial Conference on Cybersecurity is the first regional ministerial platform to bring together digital and telecommunications as well as cybersecurity ministers and senior officials from the various ASEAN member states and dialogue partners for a holistic discussion on key cybersecurity matters of concern, thus complementing the digital-focused discussions at the ASEAN Digital Ministers' Meeting.

In 2018, ASEAN ministers and senior officials meeting at the 3rd ASEAN Ministerial Conference on Cybersecurity agreed to subscribe in principle to the 11 voluntary and non-binding norms of responsible state behaviour set out in the 2015 UNGGE Report, making ASEAN the first region in the world to do so.[100] This decision was quickly followed through with an initiative to develop an ASEAN Norms Implementation Checklist and Regional Action Plan Matrix under Malaysian leadership, to serve as a reference to ASEAN member states in the implementation of the norms in accordance with their national priorities, and also as a guide to the capacity-building activities required to enable the effective implementation of these norms. The finalised Norms Implementation Checklist and Regional Action Plan Matrix are both due to be tabled for

[100] ASEAN. (2018, September 27). *Chairman's Statement of The 3rd ASEAN Ministerial Conference on Cybersecurity*. https://asean.org/speechandstatement/chairmans-statement-of-the-3rd-asean-ministerial-conference-on-cybersecurity/

approval by ministers at the 9th ASEAN Ministerial Conference on Cybersecurity, to be convened in October 2024.

ASEAN member states also established an ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) in 2020 to coordinate among the various regional workstreams and platforms dealing with national cybersecurity, cybercrime and defence-related cybersecurity. The ASEAN Cyber-CC recognises the increasing overlaps between these workstreams and seeks through its discussions to facilitate information sharing between these various ASEAN platforms and identify areas where regional policies could be better aligned, synergies could be tapped and duplications in cooperation and capacity-building efforts minimised and avoided. The ASEAN Cyber-CC also works closely with ASEAN member states and the ASEAN Secretariat to provide guidance on the planning and scheduling of cybersecurity dialogues with Dialogue Partners and seeks to ensure that the pace and scope of such dialogues are balanced and relevant to the interests of the region and the Dialogue Partners.

Deepening cyber policy exchanges with external partners

ASEAN member states have been strongly aware of the importance of pursuing cybersecurity cooperation with international partners from across the world given the transboundary nature of cyber. ASEAN as a regional grouping has long been open to such international cooperation and has

established several key mechanisms to facilitate this. One example is the ASEAN Regional Forum (ARF), which was established in 1993. The ARF is a consultative forum for the Asia-Pacific region to promote open dialogue on political and security cooperation in the region.

ASEAN member states have also continued to deepen exchanges with international partners on cybersecurity issues. Both the ASEAN Digital Ministers' Meeting and the ASEAN Ministerial Conference on Cybersecurity have dedicated components in their meeting agendas to allow for interactions with Dialogue Partner countries on cybersecurity and geopolitical developments, as well as to discuss possible joint cyber-cooperation initiatives.

At the broader level, in response to the increasingly sophisticated and transboundary cyber threats facing the region, an ARF Work Plan on Security of and in the Use of Information and Communications Technologies was established in 2015 with the intent of promoting a peaceful, secure, open and cooperative ICT environment. In 2018, an ARF Inter-Sessional Meeting on Information and Communication Technologies Security (ARF ISM on ICTs Security) was established to serve as a mechanism for the implementation of the work plan. The ARF ISM on ICTs Security and its Open-Ended Study Group (OESG) focus on the adoption of CBMs and capacity-building activities to facilitate communication, information sharing and exchange of know-how and best practices. Since its formation, the ARF ISM on ICTs Security has spearheaded some key regional initiatives including those

around CII protection, CERT-related capacity building, cybercrime cooperation and CERT-related information sharing.

The ARF ISM on ICTs Security was also instrumental in establishing an ARF Points-of-Contact Directory on Security of and in the use of ICTs in 2019 as well as the adoption of the following CBMs in the ASEAN region: (a) Sharing of Information on National Laws, Policies, Best Practices and Strategies as well as Rules and Regulations; (b) Awareness-Raising and Information Sharing on Emergency Responses to Security Incidents in the Use of ICTs; (c) Workshop on Principles of Building Security in the Use of ICTs in the National Context; (d) Establishment of ARF Points of Contact Directory on Security of and in the Use of ICTs; (e) Protection on ICT-Enabled Critical Infrastructures; (f) Workshop on Countering the Use of ICTs for Criminal Purposes; and (g) ARF Terminology in the Security of and in the use of ICTs.

In addition to increasing trust, deepening common understanding among states and avoiding the risks of misperception and escalation, the discussion on CBMs (also during the exchanges at the ASEAN Digital Ministers' Meeting and ASEAN Ministerial Conference on Cybersecurity) has served to provide the opportunity for a frank and robust exchange between ASEAN member states and international partners on the different perspectives and frameworks held by the international community on the issues related to the voluntary, non-binding rules, norms and principles of state behaviour in cyberspace, allowing each side to reach a better understanding of the other's perspectives.

ASEAN has also set up dedicated bilateral cyber dialogues with Dialogue Partner countries. Besides discussing matters of cybersecurity policy and operational cooperation, these dialogues frequently address cyber diplomacy issues. At present, five such cyber dialogues have been established.[101]

Advancing coordinated regional cyber capacity-building

Coordinated cyber capacity-building remains the cornerstone of ASEAN member states' efforts to better equip officials with the multidisciplinary skills needed for international cyber diplomacy. ASEAN Leaders in their 2018 Statement on Cybersecurity Cooperation as well as ASEAN Ministers meeting in the ASEAN Digital Ministers' Meeting and the ASEAN Ministerial Conference on Cybersecurity have very consistently underlined the importance of timely, relevant and needs-based capacity-building initiatives to ensure that member states have the necessary national capacities to effectively address and mitigate ever-evolving and sophisticated cyber threats, but also to implement the voluntary, non-binding rules, norms and principles of responsible state behaviour in cyberspace agreed to by consensus in international and regional discussions.

As with other regional cybersecurity initiatives, ASEAN cyber capacity-building efforts are designed to be inclusive, politically neutral and tailored to support ASEAN member states in

[101] These cyber dialogues have been established with China, India, Japan, Russia and the US.

building their national cyber policy, operational, technical, legal and diplomatic capacities in line with national priorities and preferred pace of development.

Another key distinctive of ASEAN regional cyber capacity-building programmes is the partnership with international government partners from Dialogue Partner countries as well as industry, academia and civil society groups. These partnerships have the advantage of ensuring that regional cyber capacity-building programmes are timely and responsive to the challenges posed by the rapidly evolving global and regional cyber-threat landscape and that the best expertise is brought to bear in the design and delivery of these programmes.

The timeliness and relevance of regional cyber capacity-building are ensured by the reviews of regional cyber capacity-building needs that is conducted as part of the five-year ASEAN Cyber Cooperation Strategy as well as more regularly through senior official-level discussions at the ASEAN Cyber-CC, ASEAN Network Security Action Council and ASEAN Regional CERT Taskforce, and ministerial discussions at the ASEAN Digital Ministers' Meeting and ASEAN Ministerial Conference on Cybersecurity.

These review mechanisms allow guidance and interventions to be given in a timely manner to ensure that regional cyber capacity building remains responsive and nimble to current capacity-building needs of ASEAN member states. For example, recent reviews have recommended that regional cyber capacity-building programmes focus on newer threats such as

ransomware and the security of emerging technologies, such as artificial intelligence (AI).

ASEAN–Japan Cybersecurity Capacity Building Centre

To better deliver these programmes, ASEAN has also set up two cyber capacity-building facilities in the region. The ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC), established in 2018 and located in Thailand, focuses on cybersecurity training for government officials and CII operators in ASEAN member states. The AJCCBC is managed by the National Cyber Security Agency (NCSA) of Thailand and the Japan International Cooperation Agency.

The centre was established with the aim to develop a cybersecurity workforce of over 700 professionals over four years to enhance the capacity of cyber experts and specialists in ASEAN member states through three courses: (a) Cyber Defence Exercise with Recurrence; (b) Hands-on Forensics; and (c) Hands-On Malware Analysis,[102] as well as other relevant workshops, seminars and exercises.

In line with the ASEAN principle of tailoring regional cyber-capacity programmes to newer emerging threats, for the years

[102] *ASEAN-Japan Cybersecurity Capacity Building Centre - CYBIL Portal*. (n.d.). Cybil Portal. https://cybilportal.org/projects/asean-japan-cybersecurity-capacity-building-centre/

2023–2027 the AJCCBC will be implementing a 'Project for Enhancing ASEAN–Japan Cyber Capacity Building Programmes for Cybersecurity and Trusted Digital Services'.

ASEAN–Singapore Cybersecurity Centre of Excellence

Singapore launched the ASEAN Cyber Capacity Programme (ACCP) in 2016 to support regional cyber-capacity efforts. Following the positive feedback from international partners and participants, Singapore announced the establishment of the ASEAN–Singapore Cybersecurity Centre of Excellence (ASCCE) in October 2019 with a commitment of S$30 million over five years, and renewed it in 2024, to conduct cybersecurity training programmes for senior ASEAN policy and technical officials. The ASCCE campus was officially opened during the 6th Singapore International Cyber Week in 2021. To date, the ASCCE and ACCP have delivered close to 60 programmes that were attended by over 1,600 senior officials from ASEAN and beyond, and collaborated with over 50 partners from across governments, private sector, academia and non-governmental organisations.

The ASCCE undertakes a modular, multidisciplinary, multistakeholder and measurable approach to deliver capacity-building programmes in three principal areas:

a. Conduct research and provide trainings in areas spanning international law, cyber strategy, legislation, cyber norms and other cybersecurity policy issues

b. Provide CERT-related technical training as well as facilitate the exchange of open-source cyber threat and attack-related information and best practices
c. Conduct virtual cyber-defence trainings and exercises.

Singapore works closely with the UN Office for Disarmament Affairs and the National University of Singapore to run the biannual UN–Singapore Cyber Fellowship. The fellowship is targeted at the heads and deputy heads of the agencies overseeing cybersecurity as well as cyber ambassadors from all UN member states. It seeks to empower participants with interdisciplinary expertise to effectively oversee national cyber and digital security policy, strategy and operations requirements. In addition to cultivating a greater understanding of the field, the fellowship serves as a platform for building relations and networking among global cybersecurity officials.

In October 2023, the SG Cyber Leadership and Alumni Programme was launched, as an extension of the ASCCE's cyber capacity-building efforts to ASEAN and beyond. The programme aims to equip officials on cyber and digital security policy, international law, strategy, operations and technical training, through training courses catered to participants at the executive, foundation and advanced levels. The programme will also include a Cyber Leaders' Alumni Fellowship and is open to all past participants of the programme. Placements for the programme will be open to AMS partners, as well as states from the Pacific Islands Forum, CARICOM and Africa. To support this new programme, Singapore's earlier funding commitment of

$23 million for cyber capacity-building will be extended by another three years, from 2024 to 2026.

Conclusion—a holistic approach to cyber diplomacy

These efforts to enhance multidisciplinary capacities, ensure cyber-policy development and coordination and foster robust and practical cooperation in the national cybersecurity domain are mirrored in the regional cybercrime discussions and initiatives under the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) and the defence-related cyber discussions at the ASEAN Defence Ministers' Meeting (ADMM).

ASEAN member states continue to see the importance of advancing the establishment of a strong rules-based, inclusive, secure, open and interoperable cyberspace and fostering robust cooperation within the ASEAN region and beyond to ensure that all countries can derive the benefits of the digital future. The ASEAN Leaders' Statement on Cybersecurity Cooperation affirmed 'the need for ASEAN to speak with a united voice at international discussions'. ASEAN member states actively participate in multilateral discussions including at the UN. At the time of writing, Singapore chairs the UN Open-ended Working Group (OEWG) on Security of and in the use of ICTs (2021–2025). ASEAN member states have remained engaged to contribute our regional perspectives to this platform and in offering concrete proposals for consideration by the global community of cyber practitioners. This includes

the Philippines' recent proposal for a needs-based cyber capacity-building catalogue, which is still being discussed within the OEWG.

Cyber diplomacy is a team effort not only because it is multidisciplinary, but also because all countries—large and small—are united in their commitment to address cyber threats that can derail our national security, economic growth and social compacts.

Even while focusing on national and regional cybersecurity policy, diplomacy and capacity-building initiatives, the outlook and aspiration of ASEAN as a region remain strongly international.

Sithuraj Ponraj

Director, International Cyber Policy Office, Cyber Security Agency of Singapore

Sithuraj Ponraj currently serves as the Director of the International Cyber Policy Office at the Cyber Security Agency of Singapore (CSA). In this role, he drives CSA's bilateral, regional and international engagements through initiatives such as the ASEAN Cyber Capacity Program (ACCP), the Singapore International Cyber Week, as well as co-chairing the ASEAN Regional Forum Open Ended Study Group on Confidence Building Measures. His key areas of focus include norms of responsible state behaviour in cyberspace, cybersecurity confidence building measures and capacity building efforts. Prior to joining CSA, Sithuraj held positions in the Singapore

Parliament, as well as the National Security Coordination Secretariat.

The Future of Cybersecurity: Embracing Multistakeholder Diplomacy

Neno Malisevic

Over the past 20 years cyberspace has become a battlefield, with governments deploying increasingly sophisticated offensive tools to undermine the stability, security and trustworthiness of the internet itself. Critical infrastructures have been and are being damaged by cyberattacks, including attacks on hospitals and vaccine suppliers during a time of pandemic. Trusted resources, such as software update mechanisms, are being targeted. Cyberespionage is an everyday occurrence. A new private sector market has even emerged where cyber mercenaries' sole focus is on undermining our networks.

This new and dynamic battlefield requires a new and dynamic response. States have struggled to evaluate and fully understand the ever-changing threat landscape and to determine what the appropriate responses would be to a cyberattack by a different country. Accountability and deterrence frameworks from the kinetic age no longer work and apply. The war in Ukraine has further blurred the lines between kinetic and cyberattacks and, indeed, between war and peace online.

To address these complex challenges, multilateralism alone is no longer enough. A new and dynamic response is required—i.e. *multistakeholder diplomacy*—which brings together all relevant parties to tackle issues too complex to be resolved by any one of them. Importantly, this approach does not imply that industry or civil society take decisions that should be taken by governments, but rather that all parties come together to ensure the stability, security and trustworthiness of the internet. It is about empowering states to take the most informed and, by extension, the best possible decisions. In essence, it is about giving civil society and industry a *voice* rather than a *vote*.

While many states support the idea of listening to non-governmental stakeholders as part of their deliberations, in practice the situation has been complex. This is especially true of the discussions at the United Nations' First Committee, where, traditionally, deliberations on cybersecurity took place among relatively small groups of states, with limited external visibility or scrutiny.

Recent UN initiatives, such as the Open Ended Working Group, have invited non-governmental stakeholders to participate. However, their participation was and is subject to approval by member states, and can be vetoed by any one state. In practice, this has prevented many of the most relevant non-governmental stakeholders from meaningfully participating in UN deliberations.

One positive example, from the UN's Third Committee, is the Ad-Hoc Committee that has been tasked to develop a UN cybercrime convention. It provides a useful baseline for what a minimum of meaningful multistakeholder participation could

look like. Moreover, states advocating for new frameworks, such as the Programme of Action, have also vowed to enable meaningful multistakeholder participation by default. But, as with all UN processes, this will be subject to negotiations.

It is worth reiterating that when it comes to threats emanating from cyberspace, neither the status quo nor the trends are particularly encouraging—unless all relevant stakeholders come together and stand up to them *together*. In this respect, multistakeholder initiatives in recent years have driven concrete action and thought leadership on key issues including *election security*, *healthcare security*, *critical infrastructure protection*, *water security* and *international law*. These can and should serve as inspiration for future multistakeholder endeavours.

As UN member states deliberate the next steps for UN cybersecurity-related discussions and actions, it is critical that they embrace and leverage the expertise and experience that non-governmental stakeholders bring to the table, especially from civil society and industry: not least because so many challenges still lie ahead—for example, the crucial issue of ensuring that states recognise cloud services as critical infrastructure, with protection against attack under international law.

Much is at stake. Threats emanating from cyberspace will continue to be one of the key challenges of our time—both present and future. In order to effectively meet these challenges, the world needs processes that listen to all relevant stakeholders, that learn from past mistakes and limitations and that leverage all available resources.

In other words, to effectively deal with cyber threats today and tomorrow, the world needs multistakeholder diplomacy.

Nemanja (Neno) Malisevic

Director, Digital Diplomacy, Microsoft

Nemanja (Neno) Malisevic joined Microsoft in 2014. He leads the company's efforts related to multistakeholder digital diplomacy – with a particular focus on cybersecurity norms. Prior to joining Microsoft, Mr. Malisevic worked more than 10 years for the Organization for Security and Co-operation in Europe (OSCE) where, he was the Organization's first Cyber Security Officer. Before that, he led the Organization's efforts dealing with combating terrorist use of the Internet. Mr. Malisevic holds a Bachelor degree (B.A) from the University of Wales (Cardiff, UK) and a Masters degree (M.Litt.) from the University of St. Andrews (St. Andrews, UK).

Cyber Diplomacy: Global Views from the South

Isaac Morales Tenorio

Today, it is difficult to imagine a multilateral discussion on cybersecurity, cybercrime or cyberspace governance without the voices of developing countries, from the smallest islands to countries with a growing economy based on digital transformation. Whether by Fiji, Costa Rica, Malaysia, Ghana, Singapore, India or Mexico, the seats in the United Nations rooms of the countries considered 'Global South' are now always occupied.

The arrival to these topics of the voices of countries that are not great cyber powers has not been linear, nor without difficulties. Like other issues on the international security agenda, in which long-term strategic vision, existing capabilities and robust diplomatic deployment concentrate the main decisions in a limited number of great powers, the issues of cyberspace initially captured the attention only of nations with high technological development or with military complexes with solid bases of innovation, alongside an understanding that these were exclusively topics for specialists with a mainly technical profile.

Nothing could be further from the truth than to think that cyberspace—a domain with few visible borders—does not matter to countries with lesser capabilities. It is precisely from these non-dominant visions that a multilateral and universal

path has been opened and accompanied by the prioritisation of issues and concerns not always present on the agenda of the great cyber powers, such as awareness of the enormous technological divide, the importance of cooperation and capacity-building programmes, and specific contributions to mechanisms for the peaceful settlement of disputes, the configuration of innovative confidence-building measures, or less offensive visions on the application of international law in cyberspace.

Tracing the path

The United Nations Group of Governmental Experts (GGE) was the starting point for the systematic multilateral discussion of cyberspace and international security around two decades ago. Considered the cradle of cyber diplomacy, the GGE marked the way in which the initial participation of countries outside the sphere of the great powers in matters of cyber dominance was configured.

Having originated within the scope and mandates of the First Committee of the United Nations General Assembly and with a composition limited to 20 or 25 experts in which the five permanent members of the UN Security Council were always present, the GGE entailed a model focused on discussions between great powers, sometimes even being seen as a space for discussion between only two conflicting visions: one considered Western, the other led by Russia and China (who, by the way, did not always agree on everything).

At the nucleus of the GGE, a community of specialists was formed, initially more focused on technical knowledge, the functioning of the technologies that enabled cyberspace and the tools to protect critical infrastructures. As the discussion deepened with a perspective of foreign policy, national security and the promotion of peace, this community became more specialist on international affairs and better endowed with diplomatic experience, and came to promote minimal but sufficient agreements to provide the UN universal membership with norms for the responsible behaviour of states or confidence-building measures that, without the implementation of the best tradition of diplomacy, would not have found a place. Seeing itself as a family, this incipient diplomatic community recognised in the US expert the mother of the rules, and the father of them in the Russian expert.

The operating model of the GGE, with dual opposing visions, led developing countries to become aware of the convenience of being represented at the cyber discussions by diplomats, experts on First Committee issues, and of the international security regimes consolidated over decades from the UN. These experts began to nourish the deliberations with different visions: visions from the middle, which gradually opened the conversations to issues closer to development, cooperation, the protection of human rights online or the precise agenda of capacity building.

Although the link between cyberspace and international security was considered a departing point for UN discussions, they were sometimes not associated with a broader vision of the First Committee, or with the progress achieved on the

margins of other peace and security processes. Diplomats from the Global South well experienced in these issues contributed to the contextualisation of some deliberations and the application of lessons (not always good) learned from negotiations in other areas of the security agenda, such as conventional weapons, outer space or the control of weapons of mass destruction. Thus, proposals on mechanisms for permanent dialogue, on the creation of an institutional body or even on the interpretation of the international responsibility of states for wrongful acts contrary to international law were expanding (and complicating) the range of proposals on the cyber-diplomatic table.

The GGE was certainly a real training exercise. Countries small in geography but with exemplary technological bases, such as Estonia or Singapore, began to add value to the thematic agendas. Meanwhile, voices of experts from countries such as South Africa, Kenya, Indonesia, Brazil and Mexico began to actively embrace positions rooted in Chapter VI (Peaceful Settlement of Disputes) and Chapter VIII (Regional Arrangements) of the UN Charter as a mean of reducing tensions and advancing even more sensitive discussions related to the application of Chapter VII of the Charter (Action with Respect to Threats to the Peace and Acts of Aggression) in cyberspace.

A key element that is not commonly recognised was the specialisation that the GGE promoted from the Secretariat. The UN Office of Disarmament Affairs (UNODA) staff and an invited support team of experts from the UN Institute for Disarmament Research (UNIDIR) and other academic and research

institutions provided the GGE members with background papers, examples or reflections in the room and even individual non-papers that emphasised specific aspects of the global cyber discussion. The degree of specialisation achieved by this community of experts was noticed very quickly and it began to be regarded by developing countries as reference voices not for the most technical aspects but for the political considerations and international law that were providing their own content to cyber diplomacy.

The support of these specialists and academics in the room, and of the staff of the Secretariat, provided the GGE experts from developing countries with tools to which one-person delegations did not have access, in contrast to the always large deployments of support staff for the experts from the developed world.

Much of the initial involvement of the Global South in shaping the practice of cyber diplomacy was due to those experts or diplomats who were part of one-person delegations, and who individually paved the way internally, upon return to their countries of origin after each session of the GGE. Even in the absence of international legally binding instruments, or universal definitions for key terms, these emerging cyber diplomats simultaneously advanced at the national level concrete efforts and basic common understandings, as if they had an obligation to actively engage in those increasing cyber deliberations.

An additional positive element that is less visible, and brought about by the mandate of the GGE, was the decision to hold the meetings between New York and Geneva. What perhaps in

geographical perspective represented balance also ended up familiarising experts from developing countries, for example, with considerations centred around the disarmament agenda in Geneva versus elements of development diplomacy and international law in New York.

Not uniform but colourful

The increasingly deep and numerous involvement of the countries of the South in discussions on cybersecurity did not represent the arrival of a uniform voice, but rather of a plurality of visions, with different priorities and understandings, but all converging on at least three affirmations: the role of multilateralism and the UN; the call for the implementation of the norms and international existing legal framework in cyberspace; and the demand to strengthen international cooperation and capacity building.

In this stage of more mature cyber negotiations and of greater interest in smaller countries being involved in them, despite the initial politicisation of the competing proposal to consider a broader and more inclusive format of discussions that finally established the OEWG, developing countries found a procedural enabler for their constant participation, and then the appropriation of the universal recognition of previous GGE commitments now necessarily need to be implemented. This idea of progressive work, of the *acquis*, contributed to substantiating many of the proposals and statements of the new, fresh cyber voices.

Diplomats not previously engaged in cybersecurity found a key source from which to gain background and clearer ideas of what cyber diplomacy was in the side events and the efforts to socialise studies or training that were more frequently organised by institutions such as UNIDIR, the Global Forum of Cyber Expertise (GFCE), DiploFoundation, the Center for Strategic and International Studies (CSIS) or Wilton Park, or by regional organisations such as the Organization of American States (OAS), the Organization for Security and Co-operation in Europe (OSCE) and the EU CyberDirect initiative. The message was then perceived more clearly from these specialised centres that the substance of the negotiations was closer to the work of the foreign ministries than to the ministries of technology or communications or defence.

It can be said that it was the international arena that led many developing countries to advance or prioritise domestic cyber agendas, from the creation of inter-agency coordination mechanisms to the development of national cybersecurity strategies or laws. When the OEWG initiated discussions, only a handful of developing countries had a national cybersecurity strategy, and almost none had any specific law or internal regulation, while today the agendas of legislative discussion on cybersecurity have become commonplace practically all over the world.

For a broader recognition of what cyber diplomacy means, it's relevant to mention that inter-agency coordination and collaboration was crucial, so that the diplomats sitting in the UN rooms did not have an isolated and empty voice. These mechanisms for international dialogue strengthened the

coordinating role of the foreign ministries in many countries, with emblematic cases in Latin America in which coordination worked in two ways: to follow up and monitor the implementation of international agreements or advancements, and at the same time to channel aspects of interest or concerns of the national implementing agencies to the multilateral sphere.

Beyond the UN, in the specific case of some regional organisations such as ASEAN, OSCE, OAS, the African Union or the European Union, robust conversations on confidence-building were triggered, which over time led to initiatives that universalised the conversation on cybersecurity at the national level. These regional approaches enriched the scope of UN discussions and sometimes contributed to accelerating the implementation of very concrete commitments, for instance the designation of points of contact and the creation of a directory. In particular cases, as in the Americas, the active programme of work on cyber issues carried out by the Inter-American Committee against Terrorism (CICTE)–OAS and the Inter-American Judicial Committee obligated member states to better capacitate their diplomats and to develop somehow their own cyber doctrine, and commit to implement agreed regional measures: even going so far—as in the case of Mexico—as to act as chair in both instances.

Also, for some countries with strong interaction in security matters with their subregional neighbours, the emergence of bilateral or sectorial dialogues demanded greater attention at the national level and the creation of specific offices or posts more specialised in cyber diplomacy. For example, in Mexico,

the bilateral dialogue with the US and trilateral dialogue with the US and Canada generated a mirror at the national level to reflect international commitments and to appropriately cover the growing attention to cyber discussions. These bilateral and trilateral talks, at the level of decision-makers, imposed internal pressure, but above all created an environment to listen more closely to consolidated positions on issues being addressed at the United Nations, which allowed Mexico to advance its own vision, in dialogue with or contrasting with others' visions.

As a result of the expanded opportunities given by international cooperation, in addition to major capacity-building programmes, countries of the South also found usefulness in fellowship and sponsored funding programmes that were offered for international meetings and by specific regional or multistakeholder bodies, especially those relating to the participation of more women, who were often almost entirely absent from the negotiating rooms in the early stages.

It is difficult to know whether the global COVID-19 pandemic stimulated the participation of the global regions in GGE and OEWG discussions or not, but through remote meetings smaller countries finally had a chance to take the floor and express their positions. Due to lack of resources and travel constraints, it was difficult to those countries to be represented in all the on-site meetings.

The urgency of the reality

All these cumulative experiences and the progressive involvement of more and more countries, organisations and stakeholders to the point of what can be considered a universal discussion have effectively generated a sense of the construction of a new international regime, which incorporates diplomats and experts in foreign policy and international security as well as technicians, making the former more like technical experts and the latter more diplomatic.

But beyond the increasing number of multilateral and regional discussions and their requests to report on implementation and progress made, the facts began to reach the foreign ministries because of the emergence of a growing trend in frequency, complexity, impact and scope of attacks and cyber risk situations that began to affect the critical infrastructure of developing countries, having previously been perceived as taking place only in the developed world. Arising from the need to have cyber diplomats, countries soon faced the need to have a cyber foreign policy.

For those countries not part of any joint military alliance, and in the absence of a norm or doctrine or strategy to declare the existence of and respond to a cyberthreat, each country has adopted its own approach and domestic procedures for incident response, usually urgently once the incident or attack was ongoing. That confirms the urgent need to recognise cyber diplomacy as an indispensable tool, both to cyber powers and to the cyber developing world, and even to build communication bridges between and among them.

The GGE norms of responsible state behaviour in cyberspace, followed by the recommendations made by the OEWG, have provided some general clues inviting states to adopt or strengthen national policies, legislation, mechanisms, structures and procedures to assess and respond to cyberthreats. But recently, the cyber diplomats attending the OEWG also began to attend the Ad Hoc Committee on Cybercrime and the discussions in the International Telecommunication Union and the Internet Governance Forum, in addition to even more specialised discussions related to emerging technologies, such as those on lethal autonomous weapons or the protection of data privacy and digital rights.

In comparison to the specialisation by forum observed in diplomats from countries with more resources, diplomats from the South with multiple representation obligations have of course faced more challenges, but paradoxically also have allowed a discursive consistency to be generated—although not always in a positive sense—which allowed parallel negotiations to advance that could be unblocked in one forum to yield in another. It also allowed the idea of a comprehensive approach, for instance, to knowing what progress was being made in cybercrime and in human rights in order to look for references that would help consolidate or implement these advances in the field of cybersecurity.

It cannot be ruled out that this incorporation of cyber diplomacy with global visions beyond the great powers will encounter new challenges in a possible dispersion of multilateral conversations and agreements, due to the growing attention on emerging technologies such as Artificial

Intelligence, or due to imprecise approaches that can expand the work and expectations of cyber diplomacy to the point of making it lose concrete meaning.

It is very significant that the developing world has appropriated what is called an international legal framework and the norms that, although agreed upon thanks to the indispensable minimums established by the cyber powers, are today starting conditions for future advances according to the cyber diplomats of the South.

It should be expected that developing countries continue to echo the calls for implementation, to institutionalise discussions and generate greater guarantees and intersectoral dialogues. They should also be the ones that most demand deliverables from multilateral discussions and that one-way visions at least be moderated. A world of rules for cyberspace is understandable for countries that find in law and diplomacy their main tools for defending sovereignty.

There is still a long way to go for the deliverables of cyber diplomacy to really respond to the urgency of the present—of the day-to-day cyber threats—but at the same time avenues are being travelled for the creation of national legislation, positions on the application of international law, or the strengthening of mechanisms for dialogue between governments and voices from the private sector, service providers, civil society organisations, and entities created by public–private partnerships.

Isaac Morales Tenorio

Senior Director for Cybersecurity and Data Privacy Communications, LATAM, FTI Consulting

Isaac Morales has 20 years of experience in cybersecurity and international security issues. He has provided strategic advice to governments, international organizations, and leading companies during cross-border negotiations, cyber crisis, and policy and regulatory issues. As Senior Director in FTI Consulting, since January 2023 he's leading the Cybersecurity practice for Mexico and LatAm. Previously, he occupied senior positions in Mexico's Ministry of Foreign Affairs, including as Coordinator General for Multidimensional Security. He was Member of the UN GGE to Advance Responsible State Behavior in Cyberspace, and served as Chairperson of the OAS Working Group on Confidence-Building Measures in Cyberspace. He was also President of the Inter-American Convention against Arms Trafficking, and member of the Confidentiality Commission of the OPCW. He represented Mexico to specialized UN, G20, OECD, INTERPOL, and FATF multilateral processes. Member of the Advisory Board of RUSI's Global Partnership for Responsible Cyber Behaviour.

Cyber Diplomacy in Latin America

Louise Marie Hurel

In recent years, Latin America has been spotlighted as a region permeated by cyber threats such as ransomware. This is not without reason: the Conti ransomware group[103] attack against the transitioning Costa Rican government in 2022 has arguably raised the profile of the region as a hotbed for ransomware-as-a-service operations.[104] While considerable attention has been paid to this incident, many other countries in the region have been suffering from the crippling effects of these threat actors but have remained less visible in international discussions on cyber diplomacy.

---

[103] Burgess, M. (2022, June 12). Conti's attack against Costa Rica sparks a new ransomware era. *WIRED*. https://www.wired.com/story/costa-rica-ransomware-conti/

[104] Insikt Group. (2022, June 14). *Latin American governments targeted by ransomware*. Recorded Future. https://www.recordedfuture.com/research/latin-american-governments-targeted-by-ransomware; Jarnecki, J., & MacColl, J. (2022, August 12). *Ransomware Now Threatens the Global South*. Royal United Services Institute. https://rusi.org/explore-our-research/publications/commentary/ransomware-now-threatens-global-south#:~:text=A%20spate%20of%20ransomware%20targeting,US%20and%20other%20G7%20members

Despite growing digitalisation in Latin America,[105] the consistent disruptiveness of recent cyber incidents has shifted from a niche inconvenience, restricted to specific cybercrime groups, to a significant vector of economic, social and political disruption. Attacks against healthcare services,[106] nuclear subsidiaries,[107] broadcasting services[108] and many other sectors have contributed to elevating (even if momentarily) the attention of political elites in the region to cybersecurity[109] resulting in pushes from countries such as Chile,[110] Brazil,[111]

[105] OECD. (n.d.). *Publications: Insights and context to inform policies and global dialogue*. https://www.oecd-ilibrary.org/sites/e7a00fd6-en/index.html?itemId=/content/component/e7a00fd6-en

[106] Abrams, L. (2022, November 30). Keralty ransomware attack impacts Colombia's health care system. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/keralty-ransomware-attack-impacts-colombias-health-care-system/

[107] Brazil's Eletrobras says nuclear unit hit with cyberattack. (2021, February 4). *Reuters*. https://www.reuters.com/article/idUSKBN2A41JM/

[108] Figueiredo, A. L. (2022, October 14). Caso Record: emissora recupera arquivos, mas ataque hacker continua. *Olhar Digital*. https://olhardigital.com.br/2022/10/12/seguranca/caso-record-emissora-recupera-arquivos-mas-ataque-hacker-continua/

[109] Hurel, L. M. (2023, April 26). *The Political Cybersecurity Blindfold in Latin America*. Default. https://www.lawfaremedia.org/article/the-political-cybersecurity-blindfold-in-latin-america

[110] La Agencia Nacional de Ciberseguridad (ANCI). (2023). *La Política Nacional de Ciberseguridad (2023-2028)*. https://anci.gob.cl/pncs-2023-2028/

[111]

Costa Rica[112] and Colombia[113] to either pass cybersecurity laws and national policies or establish national cybersecurity agencies.

There are at least four structural challenges that condition the interpretation and understanding of the emergence of cyber diplomacy in Latin America—none of which should be seen as exhaustive.

Structural challenges

Firstly, Latin America has often been portrayed as a region of relative and lasting peace[114]. While that has been the case, it is not a given nor an absolute. Throughout the past years, relations among countries in the region have faced critical bottlenecks. This includes, for example, Venezuela's move to annex Essequibo—a disputed region along its border with Guyana—in 2023[115] and Mexico severing diplomatic ties with

---

[112] Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones -MICITT. (2023). *Estrategia Nacional de Ciberseguridad 2023-2027*. https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf

[113] Red de Expertos (2024, February 16). *Las dos caras de la agencia nacional de seguridad digital*. La Silla Vacía. https://www.lasillavacia.com/red-de-expertos/red-social/las-dos-caras-de-la-agencia-nacional-de-seguridad-digital/

[114] Kurtenbach, S. (2019). The limits of peace in Latin America. *Peacebuilding*, *7*(3), 283–296. https://doi.org/10.1080/21647259.2019.1618518

[115] Wilkinson, B. (2024, April 4). *Guyana condemns Venezuela for signing into law a referendum approving annexation of disputed*

Ecuador after the police stormed into the Mexican Embassy to arrest former vice president Jorge Glas in 2024[116]—with Honduras following Mexico and recalling senior diplomats in Ecuador.[117] Moreover, presidential swings from left to right and vice versa have equally provided for a complex set of relationships and misalignments among countries in the region following waves of 'pink tides' and far-right governments in past decades.

Secondly, Latin American countries have often been associated with the 'Global South', 'Global Majority', middle ground and/or swing states. The plethora of concepts seek to grasp how these countries leverage strategic ambiguity in a polarised geopolitical landscape. Diplomatically, the resistance to the 'Global North' through collective strategic leveraging has come in different shapes and sizes. Some examples are Latin American countries' articulation with other members of the Non-Aligned Movement in areas such as telecommunications in the 1970s and 1980s;[118] Brazil, India and South Africa issuing

---

region | AP News. AP News. https://apnews.com/article/guyana-venezuela-essequibo-dispute-maduro-law-a72e94ed5417f99d090e1062c68017d7

[116] Cano, R. G., & Molina, G. (2024, April 6). *Jorge Glas, former Ecuadorian VP, has long faced corruption accusations | AP News*. AP News. https://apnews.com/article/ecuador-mexico-embassy-raid-glas-noboa-8781c998e6f684467474a159993aded4

[117] Honduras recalls top diplomat in Ecuador over Mexico embassy raid. (2024, April 16). *Reuters*. https://www.reuters.com/world/americas/honduras-recalls-top-diplomat-ecuador-over-mexico-embassy-raid-2024-04-16/

[118] Carlsson, U. (2003). The rise and fall of NWICO. *Nordicom Review/NORDICOM Review*, *24*(2), 31–67. https://doi.org/10.1515/nor-2017-0306

their first joint statement on regular institutional dialogue in July 2023 at the UN Open-Ended Working Group (OEWG) on the security of and the use of information and communications technologies; and continuous efforts from Latin American countries to informally share and align views during UN OEWG negotiations. However, greater caution should be exercised when using these concepts to examine cyber diplomacy, as they can pose an analytical risk of misreading Latin America countries' foreign policy[119] in either/or (United States or China) terms, rather than accounting for potential domestic and regional constraints. As noted previously, discourses focusing excessively on great power rivalry 'obfuscate the scope of the study of global cybersecurity politics, in general, and Latin America, in particular'.[120]

Thirdly, the emergence of cyber diplomacy in the region is contentiously linked to geo-economic disputes concerning infrastructure and technology provision—which often makes it even more challenging to break from reading Latin American (cyber) diplomacy through a bipolar geopolitical lens.[121] The advancement of cybersecurity is closely tied to Latin American countries' thirst for development. Cyber crisis assistance and

---

[119] Brun, É. (2023). The meanings of the (Global) South from a Latin American perspective. *Oxford Research Encyclopedia of International Studies*. https://doi.org/10.1093/acrefore/9780190846626.013.800

[120] Hurel, L. M. (2022). Beyond the Great Powers: Challenges for understanding Cyber operations in Latin America. *Global Security Review*, *2*(1). https://doi.org/10.25148/gsr.2.009786

[121] Pestana, R. (2023, July 24). *Cybersecurity: the next frontier of U.S.-China competition in the Americas*. Americas Quarterly. https://americasquarterly.org/article/cybersecurity-the-next-frontier-of-u-s-china-competition-in-the-americas/

capacity building has been one of the key areas for the United States' and China's investments in the region. Examples of the former include the announcement of a $25 million package of cybersecurity assistance to support Costa Rica in rebuilding and fortifying its cyber defences,[122] deployment of cyber operators in 'hunt forward' operations in Central and South America,[123] and investments in cyber and digital infrastructure through USAID's Digital Connectivity and Cybersecurity Partnership.[124] China, on the other hand, has become the region's biggest trading partner, with 22[125] countries from the region having signed on to the Belt and Road Initiative (BRI).[126] Additionally, decades-long relationships between big Chinese tech companies such as Huawei and ZTE and countries in the region

---

[122] U.S. Embassy in Costa Rica. (2023, March 29). *United States announces $25 million to strengthen Costa Rica's cybersecurity - U.S. Embassy in Costa Rica*. https://cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity/

[123] Pomerleau, M. (2023, June 8). US Cyber Command conducts 'hunt forward' mission in Latin America for first time, official says. *DefenseScoop*. https://defensescoop.com/2023/06/08/us-cyber-command-conducts-hunt-forward-mission-in-latin-america-for-first-time-official-says/

[124] *U.S. Support for Digital Transformation in Latin America and the Caribbean - United States Department of State*. (2020b, November 10). United States Department of State. https://2017-2021.state.gov/u-s-support-for-digital-transformation-in-latin-america-and-the-caribbean/

[125] Wang, C. N. (n.d.). *Countries of the Belt and Road Initiative (BRI) – Green Finance & Development Center*. https://greenfdc.org/countries-of-the-belt-and-road-initiative-bri/

[126] Roy, D. (2025, January 6). China's growing influence in Latin America. *Council on Foreign Relations*. https://www.cfr.org/backgrounder/china-influence-latin-america-argentina-brazil-venezuela-security-energy-bri

have paved the way for the former's growing presence in digital infrastructure provision.[127] Other players, such as the European Union, established a competence centre for Latin America and the Caribbean (LAC4) in 2022 with the aim to enhance cyber capacity-building projects throughout the region.[128]

Taken together, these variables—although not exhaustive—compose the landscape in which diplomatic relations between Latin American countries have and will continue to unfold.

Cyber diplomacy in the region

There are many potential recent histories of the development and emergence of cyber diplomacy in Latin America. As this section highlights, cyber diplomacy is a double movement between domestic (e.g. ensuring greater representation of cybersecurity within ministries of foreign affairs) and external dynamics (e.g. creating space for integration in cyber affairs through regional bodies and/or voluntary initiatives from countries in this area).

---

[127] Malena, J. (n.d.). The Extension of the Digital Silk Road to Latin America: Advantages and Potential Risks. *Pontificia Universidad Católica Argentina*. https://cdn.cfr.org/sites/default/files/pdf/jorgemalenadsr.pdf; Jorge-Ricart, R. (2021, April 21). *China's digital Silk Road in Latin America and the Caribbean - Elcano Royal Institute*. Elcano Royal Institute. https://www.realinstitutoelcano.org/en/commentaries/chinas-digital-silk-road-in-latin-america-and-the-caribbean/

[128] Estonians power up Latin America's cyber competence. (2022, July 20). *e-Estonia*. https://e-estonia.com/estonians-power-up-latin-americas-cyber-competence/

In recent years, the thematic rapprochement between cybersecurity and ministries of foreign affairs has taken different forms. Most of the countries in the region have incorporated international cybersecurity as part of existing departments. Others, such as Brazil, have devised new departments solely focused on cybersecurity and related thematic areas, and appointed both a 'cyber diplomat' and a 'tech envoy'.[129]

Regionally, the Organisation of American States (OAS) has been one of the key regional bodies convening discussions on cyber diplomacy. For over a decade, the Cybersecurity Programme has been organising multiple capacity building efforts to member states—which include activities ranging from trainings to support with establishing national Computer Security Incident Response Teams (CSIRTS) and National Cybersecurity Strategies.

However, two initiatives stand out as the regional body's direct contribution to intra-regional dialogue on cyber diplomacy. The first of these was the establishment of the OAS Cyber Confidence Building Measures (CBMs) working group in 2017. Since its establishment—and as highlighted in depth in Kerry-Ann Barrett's essay in this volume—OAS member states have agreed on 11 CBMs which include voluntary commitments such as designating points of contact for cyber diplomacy in foreign ministries, strengthening capacity building, and identifying a

[129] Hurel, L. M. (2023a). Mapping state actors and policies. In *Centrolatam.Digital*. https://centrolatam.digital/wp-content/uploads/2023/04/Mapping-Cyber-Policy-in-Latin-America_-The-Brazilian-Case-2.pdf

national point of contact to discuss hemispheric cyber threats.[130] The second was the OAS Inter-American Judicial Committee's 'Improving Transparency Initiative'—a project established in 2018 to map and identify areas of convergence and divergence on how states in the region see the applicability of international law to cyberspace.[131] The Initiative produced five reports on the topic based on a questionnaire and meetings seeking to address the following topics: the application of existing international legal rules and principles; a prohibition on the use of force and the right of self-defence; state responsibility for non-state actors; international humanitarian law; sovereignty; and due diligence. Some of the key takeaways were:[132]

- Unevenness in how states prioritise, develop expertise and organise responsibility within the government to deal with such agendas

---

[130] The Organization of American States (OAS). (n.d.). *WORKING GROUP ON COOPERATION AND CONFIDENCE-BUILDING MEASURES IN CYBERSPACE*. https://www.oascybercbms.org/

[131] Hollis, D., & Vila, B. (2020, July 29). Elaborating International Law for Cyberspace. *Directions Blog*. https://directionsblog.eu/elaborating-international-law-for-cyberspace/

[132] Correa Palacio, R. S., García-Corrochano Moyano, L., Bandeira Galindo, G. R., Bertrand Galindo Arriagada, M., Espeche Gil, M. Á., Hollis, D. B., Moreno Rodríguez, J. A., Richard, A., Rudge, E. P., Salazar Albornoz, M., & Salvador Crespo, Í. (2020). Inter-American Juridical Committee: International Law and State Cyber Operations. In *OAS. Official records*. Department of International Law of the Secretariat for Legal Affairs of the Organization of American States (OAS). http://www.oas.org/en/sla/iajc/docs/International_Law_and_State_Cyber_Operations_publication.pdf

- States in the region recognise that international law applies to cyberspace but with little indication as to how it applies.
- Not all states agree that international legal regimes (e.g. international humanitarian law, self-defence, countermeasures and other) apply in their totality, while others differ on how to interpret the application of rules
- The challenge of applying international law to cyberspace derives from the absence of 'tailor-made rules and standards' (e.g. no specific treaty on cyber).

Since the 2020 fifth and final report of the Inter-American Juridical Committee (IAJC),[133] two countries—Brazil and Costa Rica—have published their views on the matter, in 2021 and 2023 respectively. While extensive coverage of these positions is beyond the scope of the current essay, scholars in international law have argued that the two countries converge and diverge in their views.[134] They converge in categorising sovereignty as a rule that can be breached by other states' cyber operations and diverge on what would constitute a violation of sovereignty, with Brazil including interception of communications[135] and Costa Rica considering that 'cyber operations cause physical damage or loss of functionality of cyber infrastructure located in the victim State, regardless of

[133] ibid.
[134] Hollis, D. (2023, August 28). A Victim's Perspective on International Law in Cyberspace. *Lawfare*. https://www.lawfaremedia.org/article/a-victim-s-perspective-on-international-law-in-cyberspace
[135] *National position of Brazil (2021)*. (n.d.). The Cyber Law Toolkit. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Brazil_(2021)

ownership'.[136]

Future reflections: cyber diplomacy beyond the UN

As the previous section has highlighted, regional mechanisms such as the OAS have played an important role in consolidating specific understandings of responsible behaviour in cyberspace within Latin America. However, the future of research on cyber diplomacy in Latin America would benefit from deeper reflections on cyber diplomacy beyond the context of the UN, as it focuses on international peace and security. Other areas of investigation could cover analyses of existing and emerging memorandums of understanding (MoUs) among countries in the region and how cyber is/has featured in these agreements, the growing role of cyber crisis assistance in shaping cyber capacity building, and other regional and multilateral mechanisms covering trade and commerce—as they have increasingly sought to include cybersecurity as part of the agenda.[137]

---

[136] *National position of Costa Rica (2023)*. (n.d.). The Cyber Law Toolkit. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Costa_Rica_(2023)

[137] See Albornoz, Mariana S. (forthcoming), 'Perspectives from Latin America', in Hurel, Louise Marie (ed.), *Global Compendium on Responsible Cyber Behaviour* (London: RUSI).

Louise Marie Hurel

Cybersecurity Researcher, Royal United Services Institute

Louise Marie Hurel is a researcher working at the intersection between technology, cybersecurity and geopolitics. Her research focuses on cybersecurity as it relates to expertise, private governance, diplomacy, capacity building, development, and emerging threats. She is a research fellow at the Royal United Services Institute's (RUSI) Cyber Team and a PhD candidate at the London School of Economics and Political Science (LSE). Throughout the past decade, Louise has coordinated Igarape Institute's Digital Security Programme, has founded the Latin American Cybersecurity Research Network (LA/CS Net) and has advised specific agencies of the United Nations on data and cyber security, contributed to the work of the World Economic Forum Global Risks Report and has provided multiple research-based talks to governments, companies and scholars. She has published has been featured in both mainstream and specialised media outlets such as the Foreign Affairs Latin America, Agence France-Presse, Council on Foreign Relations, Lawfare Media, Americas Quarterly, Open Democracy and journals such as the Journal of Cyber Policy. Her work has also been cited in official national cybersecurity strategies and international organisations' reports. In 2023, Louise was nominated as a 35 under 35 Future Leaders by CIDOB-Santander.

Part 3

SELECTED NATIONAL PERSPECTIVES

Establishing a Cyber Programme of Action at the UN: Five Lessons Learned from Ongoing Efforts

Léonard Rolland

In 2020, France and Egypt along with a cross-regional group of 60 states submitted a first non-paper on establishing a Cyber UN Programme of Action (PoA) as a permanent, flexible and action-oriented platform to advance responsible state behaviour in cyberspace. As part of the cyber Open Ended Working Group (OEWG) discussion item on future 'regular institutional dialogue', these efforts aim at nothing less than bringing about a much-needed institutional reform of cybersecurity governance at UN level. While still ongoing, they already give us five valuable teachings that may be useful for a cyber diplomat freshly entering the UN arena, as follows.

Look for concrete solutions

As the world is becoming more complex, diplomats have their work cut out. This means they may not have time to lose on diplomatic initiatives that would not directly aim at solving problems. Therefore, rather than a discussion space only, the PoA aims to offer an action-oriented platform meeting two

frequently indicated needs: (i) we must collectively deepen our understanding of norms of responsible behaviour and keep the normative UN *acquis* updated, and (ii) we must boost our capabilities to implement these norms, through capacity building. With that in mind, the PoA will organise its work along tangible policy objectives: protecting critical infrastructure, dealing cooperatively with cyber incidents, enhancing accountability, etc.

Be inclusive 'by design'

As the proverb goes, *'If you want to go fast, go alone. If you want to go far, go together.'* I will elaborate further on the issue of time management, but the main point here is: inclusivity is not a slogan, but a recipe for success. Therefore, it was key from the beginning to extend an invitation to join our coalition in support of the PoA to a broad set of countries, beyond the usual 'like-minded' group. Inclusivity does not mean only listening to others, but also and more importantly being willing to take their views on board. What does it mean in practice? Numbers speak volumes: it took 120 bilateral meetings to lead to the adoption of our last UN General Assembly (UNGA) resolution on the PoA, by 161 votes!

Navigate geopolitical fault lines

As a 'balancing power', France has always actively looked to overcome bloc mentality. This is also true when it comes to cyberspace governance, where a strong multilateralism is

needed instead of more fragmentation, which would inevitably lead to more instability. The dual-track split between a UN Group of Governmental Experts (GGE) and an OEWG in the years 2019–2021 underlined the need to 'reunite' the process in a single and permanent track of negotiation such as the PoA. That being said, one has to acknowledge that cyber is far from a neutral topic in current geopolitical tensions. The war of aggression—of which cyber warfare is a component—launched by Russia against Ukraine in 2022 in blatant violation of the UN Charter, coupled with its attempt to whitewash its behaviour by actively promoting a new cyber treaty, is a stark reminder that not everyone thinks of the UN as a tool to increase cyber stability at global level.

Be patient …

PoA discussions started more than five years ago. That may lead to frustration for some, or to claims by others that the initiative would indeed be an 'empty shell'. In reality, the step-by-step approach is dictated by two key considerations: a willingness to co-construct the substance of the future PoA in a cross-regional manner and a willingness not to undermine the OEWG as the ongoing format. Hence our constant and constructive engagement within the group to promote and elaborate the PoA as its successor. Simultaneously, we engage with partners from all regional groups to brainstorm collectively and produce papers aimed at 'putting flesh on the bones' of the PoA.

… but ask for deadlines

While being patient, one still has to strike while the iron is hot—and by the same token prevent delaying strategies by competing actors. Since it was key to preserve the integrity of the OEWG as the current format of negotiation, we therefore suggested that the future mechanism be established no later than 2026, i.e. after the conclusion of the OEWG: a timeline that was then endorsed by the UN General Assembly in this year's PoA resolution. Having such a clear course agreed by a majority of states gives predictability to our future efforts and makes it easier for all to focus on the substance of the future mechanism.

Léonard Rolland

Head of International Cybersecurity Policies, Ministry of Foreign Affairs, France

Léonard Rolland is the Head of International Cybersecurity Policy at the French Ministry of Foreign Affairs. He started to work on cyberdiplomacy in 2013 and was a French Expert during the negotiations leading to the cyber GGE report of 2015. He has also been serving as a political adviser at the French Embassy in Moscow and then in Berlin, where he covered security-related issues, including cyber.

The views expressed in this essay are solely those of the author and do not necessarily reflect the views and mandate of the French Ministry of Foreign Affairs.

Cyber Deterrence: Underpinning Responsible Behaviour and Norms in Cyberspace

Kathryn Jones

Since the inception of the UN cyber debate, the UK has been closely involved in development of the Framework for Responsible State Behaviour in Cyberspace. Following the 2017 WannaCry attack, there was recognition of the need to look again at the ways in which we hold accountable those conducting malicious cyber activity. In doing so we made a fundamental contribution to the developing art of cyber diplomacy in the form of cyber deterrence.

Cyber deterrence is the mechanism by which we discourage actors—from nation states to cybercriminals—from carrying out malicious activities in cyberspace. The security and resilience of our infrastructure has long proved to be the best way to deter states from carrying out malicious cyber activities against us. So-called *'deterrence by denial'* relies on increasing the cost and lowering the chance of success through strong cybersecurity and resilience measures that shield us from specific malicious activity and enable a quick recovery.

But no matter how much we raise our defences; they remain vulnerable to the most sophisticated attacks. '*Deterrence by*

punishment' aims to raise the cost of a potential attack by imposing effective consequences, thus altering the risk calculus of an attacker. In combination, deterrence by denial and punishment proves a formidable and daunting challenge to any potential attacker.

If we are to counter the most destructive, disruptive and destabilising malicious cyber activity, we must underpin responsible behaviour and norms in cyberspace with an effective approach to cyber deterrence.

The tools available to states for cyber deterrence, and the considerations to take into account around using them, are broadly similar to those in any other diplomatic arena. To deploy cyber deterrence measures effectively, the UK follows a three-step process:

- First, we aim to understand the threat, gaining consensus on the risk posed to national interests
- Second, we build a coalition and garner support for a consolidated and unified response to counter the specific threat. As cyberspace is essentially borderless, any actions taken will be most effective when countries work together, coordinating their responses and actions
- Third, we build a package of costs to change the behaviour of adversaries and deter future threats through coordinated action with allies—this could include public attribution, demarches and sanctions.

This activity will be based on and/or support a high-confidence technical attribution underpinned by intelligence, which

confirms the identification of whoever is responsible for the malicious activity. This technical attribution may involve cooperating with a likeminded group or close allies, sharing intelligence, or engaging private sector expertise. This is often a painstaking and difficult process involving months of work.

The growth of an international coalition for collective action over time is clear**.** The UK's first attribution statement in 2018, of WannaCry, was made alongside four partners. A March 2024 attribution of Chinese state-affiliated actors was joined by four other countries and supported by 18 partners globally. The largest coalition so far was achieved in 2021, when 39 partners publicly called out China for broad patterns of malicious cyber activity, including the Microsoft Exchange Server attacks. Importantly, the growth of coalitions is facilitated by recognising that states may not all adopt the same approach. Each state must decide how to support an attribution in the manner best suited to their national interests and in line with their own political appetite.

The UK's national cyber sanctions regime was developed to provide a particular method of imposing cost, and came into force in December 2020. Individuals and entities can only be subject to sanctions if the UK considers that the evidence provided meets the legal threshold of a sufficiently solid factual basis. However, the UK sanctions regime is a tool separate to law enforcement processes, making it different from but complementary to, for instance, US indictments. UK cyber sanctions are only used where the perpetrator is beyond the effective jurisdiction of UK legal mechanisms. A number of

individuals and organisations from a range of countries have been designated under this regime.

Wherever the international community takes the discussion of responsible state behaviour in cyberspace next, accountability will remain crucial.

Currently the UK's focus on accountability and imposing costs remains on malicious cyber activity that falls short of armed attack. Our approach requires that our actions must be proportionate and consistent with international law, and we are clear on the objective behind any consequences we impose for malicious cyber activity, ensuring it is driven by our commitment to peaceful resolution. But for the UK, the step towards public legal attribution of cyber activity coordinated with international partners is yet to come.

As the discussion develops, we recognise that cyber deterrence must too. Whether to overcome the challenge of measuring and publicly demonstrating behaviour change over time in predominantly covert actors, to link that to clear cementing of international norms around responsible state behaviour in cyberspace, or to protect the sanctity of independent technical attribution as more states aspire to develop attribution capabilities, there is much to be done to further develop this emerging discipline.

Kathryn Jones

Head of International Cyber Governance, UK Foreign, Commonwealth and Development Office

Kathryn Jones is Head of International Cyber Governance at the UK Foreign, Commonwealth and Development Office. Her role sees her leading delegations to the UN Open Ended Working Group on Developments in the field of information and telecommunications in the context of international security and the Organisation for Security and Cooperation in Europe (OSCE) Informal Working Group on Cybersecurity, as well as taking her place on the 2021 UN Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security. She has previously worked in a range of government departments including the UK's Department for Digital Policy and National Cyber Security Centre, and has represented the UK in the OECD and the UN ITU.

India's Cyber Diplomacy Shapes Its Rule-Maker Aspirations

Sameer Patil

As the world's largest digital democracy, India has prioritised strengthening its defences against the growing cyber threats over the past few years. Domestically, it has undertaken a series of initiatives to build cyber resilience. Externally, it is building robust bilateral partnerships with other countries and expanding its participation in multilateral cyber-related forums. These efforts in cyber diplomacy also reflect India's deeper involvement in shaping the global tech regime, where it has actively put forth its perspective on emerging and critical technologies. This approach stems from a desire to avoid past experiences like those with the nuclear non-proliferation regime. Now, India aspires to be a rule-maker than a rule-taker.

In doing so, New Delhi has strongly emphasised 'digital sovereignty'. It recognises the value of open and safe cyberspace but acknowledges the potential security risks and the need to maintain its ability to defend against cyberattacks. In addition, it recognises that international cyber cooperation will remain deadlocked for the foreseeable future due to the polarisation caused by the emergence of the antagonistic Eastern bloc led by China and Russia and the Western bloc led by the US and Europe. India also recognises its unique

positioning as a 'bridge-builder', between not just these two blocs but also the Global North and the South. Therefore, New Delhi has not only prioritised working with like-minded partners but also engaged partners from the Global South on a range of issues that offer opportunities for information-sharing and skills and capacity building. This essay unpacks the various engagements that New Delhi has taken to advance its cyber diplomacy.

Cooperation with the US and its impact on India's cyber diplomacy

In 2016, India signed one of its first bilateral cybersecurity agreements with the US. The 'Framework for India–US Cyber Relationship' established a strong foundation for increased collaboration between the two countries.[138] It allowed them to tackle shared cyber threats and work together to develop a unified approach at the global level. This deepening cyber partnership also triggered several ripple effects. It altered India's approach to issues such as internet governance. India's position initially aligned with Russia and China's preference for a state-controlled model for internet governance. However, later, in a shift, it endorsed the US's multistakeholder model for

[138] Ministry of External Affairs, Government of India (August 2016). *Framework for the U.S.–India Cyber Relationship.* https://www.mea.gov.in/Portal/LegalTreatiesDoc/US16B4110.pdf

the management of ICANN.[139] True to its image as a 'bridge-builder', New Delhi has also had partial success in convincing Russia and China to support the multistakeholder model: the Brazil, Russia, India, China and South Africa (BRICS) grouping through successive declarations between 2015 and 2018 emphasised the need to involve relevant stakeholders in the evolution and functioning of the internet and its governance.[140]

Secondly, cyber cooperation with the US paved the way for establishing similar agreements with US allies such as Japan, France and Australia, where cooperation has extended beyond cyber to cover other critical technologies such as robotics, artificial intelligence and quantum. In particular, cyber cooperation with Australia has thrived with the alignment of India's cyber diplomacy and Australia's focus on the cyber-resilient Indo-Pacific.[141] The two countries hold an annual foreign ministerial level dialogue on cyber and have established

---

[139] ICANN. (2015, June 15). *Indian Government Declares Support for Multistakeholder Model of Internet Governance at ICANN53*. https://www.icann.org/en/announcements/details/indian-government-declares-support-for-multistakeholder-model-of-internet-governance-at-icann53-22-6-2015-en

[140] Patil, S. (2018, 15 August). India's lead on cyber space governance. Gateway House. https://www.gatewayhouse.in/india-cyber-space-governance/

[141] Ministry of External Affairs, Government of India (2020). '*Framework Arrangement on Cyber and Cyber-Enabled Critical Technology Cooperation between the Republic of India and the Government of Australia*.' https://www.mea.gov.in/Portal/LegalTreatiesDoc/AU20B3708.pdf

a well-endowed multi-year grant for facilitating research on cyber and other critical technologies.[142]

Thirdly, it has facilitated India–US engagement at the minilateral and plurilateral levels. For instance, both countries are part of the Quadrilateral Security Initiative (the Quad), which has primarily focused on tech cooperation. Quad's cyber initiatives include the Quad Senior Cyber Group, which looks at developing cyber resilience in the Indo-Pacific by developing basic cybersecurity principles and capacity-building projects.[143] Likewise, India is part of the US-led Counter Ransomware Initiative, where New Delhi leads the Resilience Working Group.[144]

India's positioning as a rule-maker at the multilateral level

While major power differences impede progress in cyberspace management, exemplified by the collapse of the Group of Governmental Experts (GGE) process in 2017, India has taken a

---

[142] Australian High Commission, New Delhi. (2021). *Australia–India Cyber and Critical Technology Partnership: Grant Round 2*. https://www.dfat.gov.au/international-relations/australia-india-cyber-and-critical-technology-partnership-aicctp-grant-round-2

[143] National Security Council Secretariat (2021, 31 January). 'Quad Senior Cyber Group Meets in New Delhi to Strengthen Cybersecurity Cooperation.' https://pib.gov.in/PressReleasePage.aspx?PRID=1895073

[144] International Counter Ransomware Initiative (2024). *About the CRI*. https://counter-ransomware.org/aboutus

pragmatic approach, aiming to make progress on these issues by any available means. This rationale led India to endorse both Resolution 73/27 and Resolution 73/266 in December 2018, which established the Open-Ended Working Group and the GGE 2019–21 processes, respectively.[145] At these and related UN forums, India has emerged as a strong advocate for responsible state behaviour in cyberspace. This perspective stems directly from its experience of facing cross-border cyberattacks from adversarial neighbours and the hacking groups supported by them over the past few years. India's foreign secretary, Harsh Shringla, emphasised this point during a UN Security Council debate in June 2021, stating that 'some States are leveraging their expertise in cyberspace to achieve their political and security-related objectives and indulge in contemporary forms of cross-border terrorism.'[146] Therefore, India has urged the UN to develop norms for responsible state conduct in cyberspace.

India has also called for a common understanding among member states on key concepts such as cyber sovereignty, deterrence and the nature of cyberattacks. Additionally, it highlights the importance of clear attribution and legal frameworks to maintain stability in cyberspace. India maintains

[145] Patil, S. (2018, 15 August). India's lead on cyber space governance. Gateway House. https://www.gatewayhouse.in/india-cyber-space-governance/

[146] Permanent Mission of India to the UN, New York (2021, June 29). *UN Security Council Open Debate on Maintenance of International Peace and Security: Cyber Security*: *India Statement by H.E. Mr. Harsh Vardhan Shringla, Foreign Secretary of India*. https://pminewyork.gov.in/IndiaatUNSC?id=NDI5NA

that while international law extends to cyberspace, it falls short in addressing critical concerns such as attribution, breaches of sovereignty, and the criteria for invoking the right to self-defence. Specifically, New Delhi advocates for the right to self-defence against state-sponsored cyberattacks.[147]

Besides seeking to shape norms for cyberspace management, India has also made significant efforts to utilise multilateral forums for capacity-building and information exchanges. At the Global Forum on Cyber Expertise, India has actively shared the best cybersecurity and data protection practices with other countries.[148]

Shaping the relationship with the Global South

Another evolving facet of India's cyber diplomacy has been its tech engagement with the Global South countries, under which New Delhi has offered its technical and technological expertise

---

[147] Permanent Mission of India to the Conference on Disarmament, Geneva, Ministry of External Affairs. (3 June 2019). *Statement delivered by India at the Organisational Session of the Open-Ended Working Group (OEWG) on 'Developments in the field of Information and Telecommunications in the context of International Security' in New York on June 3, 2019*.
https://pmindiaun.gov.in/Cdgeneva/statement_content/NDA2

[148] Ministry of Electronics & Information Technology, Government of India (2018, January 19). *MEITY launches Cyber Surakshit Bharat to Strengthen Cybersecurity*.
https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1517238

to develop cyber resilience and promote technology for national development.

India has actively shared its cybersecurity expertise with countries such as Vietnam, Bangladesh and Morocco. This includes establishing Centres of Excellence in cybersecurity across different nations. Additionally, India offers cybersecurity training programmes through its overseas aid initiative, the Indian Technical and Economic Cooperation Programme. Another aspect that New Delhi has emphasised is information-sharing for cyber-criminal investigations. In 2023, it hosted several global convenings where Indian officials underlined that information-sharing is critical for timely action against cyber and other new-age crimes. While India doesn't endorse the Budapest Convention, media reports have previously noted that it was reconsidering its position.[149]

India's successful implementation of the Digital Public Infrastructure (DPI) offers a high-impact, low-cost tech model for developing digital economies as they embark on harnessing tech for national development. This approach aims to empower these economies beyond simply providing technology (like the traditional aid model from the Global North to Africa and Asia). Instead, India has focused on helping these countries to build their own capacity to innovate, adapt and implement open-source technologies. During its G20 presidency in 2023, India made DPI a core element of its offering to other countries. Its

[149] Tripathi, R. (2018, January 18). *Home Ministry pitches for Budapest Convention on cyber security*. https://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber-security-rajnath-singh-5029314/

significance was further enhanced when the G20 digital economy ministers meeting in August 2023 recognised DPI as an accelerator of the Sustainable Development Goals.[150]

To sum up, India recognises that the broader geopolitical dynamics in cyberspace will impede the achievement of meaningful progress on strengthening cybersecurity. However, cooperation is still required to tackle the expanding cyber threat landscape and technological advancements. Indian cyber diplomacy has worked with this imperative to collaborate with major digital powers, offer normative inputs on global cyberspace management and shape cyber and tech partnerships with the Global South.

Dr. Sameer Patil

Senior Fellow at Observer Research Foundation

Dr. Sameer Patil has a decade-long experience in the cyber policy field. His research has spanned diverse issues such as critical infrastructure protection, cyber espionage, securing digital payment systems and ransomware as a threat to digital economy. His recent research has focused on cyber hygiene and digital civics as key enablers for developing cyber resilience. At

[150] United Nations Development Programme (2023, August 19). *G20 Digital Ministers Recognize Digital Public Infrastructure as an Accelerator of the SDGs*. https://www.undp.org/india/press-releases/g20-digital-ministers-recognize-digital-public-infrastructure-accelerator-sdgs

ORF, his work focuses on the intersection of technology and national security, including cybersecurity. He has previously worked at the National Security Council Secretariat, Government of India, New Delhi and Gateway House: Indian Council on Global Relations, Mumbai. Dr. Patil is the author of Securing India in the Cyber Era (Routledge, 2022) and has co-edited The Making of a Gelobal Bharat (Har-Anand, 2024) and Moving Forward EU-India Relations: The Significance of the Security Dialogues (Edizioni Nuova Cultura, 2017).

Feminist Foreign Policy meets Cyber Diplomacy

Regine Grienberger

Feminist Foreign Policy (FFP)[151] is based on a universalist approach to human rights and gender equality. The rights of women and marginalised groups, as well as their consistent observance and development, are at the centre of feminist politics. The rejection of the use of force and the humanitarian tradition of disarmament and arms control also underpin feminist foreign policy, which also focuses on human security rather than territorial security. These principles are also very relevant to cyber diplomacy, which main goal is to maintain a stable, secure and global cyberspace.

The gender dimension of cyberspace

The concept of gender equality acknowledges that individuals have differing needs and resources but deserve equitable treatment without discrimination. A feminist approach emphasizes intersectionality, addressing multiple discrimination categories simultaneously to reshape power dynamics, ensuring fair participation and sustainable peace.

[151] Federal Foreign Office of Germany. (2023). *Feministische Außenpolitik gestalten: Leitlinien des Auswärtigen Amts*. https://feministischeaussenpolitikgestalten.org/papers/Leitlinien_Feministischer_Au%C3%9Fenpolitik.pdf

Feminist cyber diplomacy builds on this by recognizing the specific impacts of technology on women and vulnerable groups globally. Women often face restricted access to physical and digital spaces due to systemic inequalities. For instance, International Telecommunication Union (ITU) data reveals that 69% of men use the internet globally compared to 63% of women, reflecting broader societal disparities. An Amnesty study from 2017 identified anonymity online as a problem; 59% of women affected by online violence stated that it came from strangers.[152]

Implementing FFP principles in cyber diplomacy

Feminist cyber diplomacy emphasizes incorporating a gender dimension into cyber security and capacity-building efforts. Three key areas for action include:

1. Increase the Representation of Women

Women's underrepresentation in STEM and decision-making roles stems from systemic barriers and societal norms that limit their participation. Feminist cyber diplomacy seeks to address this disparity by advocating for increased representation and meaningful participation of women. This is essential to

[152] Amnesty International. (2017, November 20). *Amnesty reveals alarming impact of online abuse against women* [Press release]. https://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

integrate diverse perspectives into decision-making processes and redefine cyber security strategies.

First steps include gender-specific data collection to go beyond stereotypes and accurately measure progress. Without reliable data, systemic issues remain unaddressed.

Empowerment programs are equally critical. Initiatives like ITU launched "Her Cyber Tracks," the European "Women4Cyber"[153] network, and the UN 1st Committee "Women in Cyber Fellowship" are excellent examples of gender-transformative projects fostering women's visibility, technical expertise, and leadership in cybersecurity fields. These programs help ensure that women's voices are heard in multilateral negotiations and decision-making spaces.

Women's involvement is also crucial for integrating gender perspectives in cyber peace processes, consistent with UN Security Council Resolution 1325, which emphasizes inclusive peace negotiations.[154]

2. Strengthen the Rights of Women

The digital era has added new dimensions to gender-based inequality. The prevalence of gender-based violence online highlights the urgency of extending women's rights and protections to the virtual realm.

---

[153] Women4Cyber. (n.d.). *About Us- Women4Cyber*. https://www.women4cyber.eu

[154] *Landmark resolution on Women, Peace and Security (Security Council resolution 1325)*. (n.d.). https://www.un.org/womenwatch/osagi/wps/

A staggering 38% of women experience gender-based online violence, with specific groups like female journalists and parliamentarians particularly vulnerable. Digital spaces amplify risks due to their scale, anonymity, and speed. Addressing these issues requires tackling structural inequalities and the unique vulnerabilities introduced by technology, such as male-normative design biases in virtual reality and "femvertizing."[155] AI applications in cyberattacks, such as AI-generated phishing targeting feminist figures, demonstrate the urgency of addressing gender biases in algorithm design. States must fulfil their duty to protect women's rights online, eliminating blind spots through better data collection and multi-stakeholder collaboration with civil society and academia.

In conflict scenarios, the stakes are even higher. Cyberattacks preceding physical hostilities disproportionately impact women, yet research on gender-specific consequences in cyber warfare is sparse. Including a cyber component in the "Women, Peace, and Security" agenda would ensure that women are involved in peace negotiations addressing both physical and digital threats.

3. Mobilize Resources from and for Women

Resource inequality is a significant barrier to women's participation in secure digital transformation. Feminist cyber

[155] Millar, K., Shires, J., & Tropina, T. (2021). *Gender Approaches to Cybersecurity: design, defence and response*. https://doi.org/10.37559/gen/21/01

diplomacy must identify avenues to redistribute resources and foster gender-sensitive projects.

Targeted funding mechanisms are essential, with gender-transformative projects prioritized in cyber capacity building. For example, education and care facilities—critical for women's participation in the workforce—should be included in the definition of critical infrastructure and receive appropriate cybersecurity measures.

Cyber diplomacy must also address systemic biases in resource allocation, ensuring equitable access to digital tools and protections as an element in the capacity building programmes. By mobilizing support from governments and international organizations, it is possible to create a more inclusive and resilient cyberspace for all.

Outlook

Feminist foreign policy is a framework for action that emphasizes the integration of gender perspectives across all domains, making it particularly relevant to cyber diplomacy. Since cyber security inherently has a gender dimension, so must cyber diplomacy. Countries such as Germany, Canada, and Chile have shown leadership in this area, offering opportunities for international collaboration. One urgent area for joint action is artificial intelligence, where discriminatory biases in algorithms amplify existing inequalities and cyber threats are increasingly sophisticated. For example, AI-driven attacks, such as the Iranian case targeting feminists via phishing emails,

underscore the dual challenges of gender discrimination and cyber security. As Cathy O'Neil aptly stated, "Algorithms are opinions embedded in code," meaning AI systems often reflect and perpetuate societal biases. Addressing these compounded challenges requires mainstreaming gender sensitivity in AI development and cyber diplomacy to foster a more inclusive and equitable digital future.

Dr. Regine Grienberger

Former Cyber Ambassador, Federal Foreign Office of Germany

Regine Grienberger studied agricultural sciences at the Technical University of Munich and in Bonn and worked for the AgraEurope press agency until 2000. She has been a diplomat at the Federal Foreign Office since 2001. After working in the European Department, Communications Department and at the embassies in Ljubljana and Rome, she became Deputy Head of the Minister's Office under Federal Foreign Ministers Sigmar Gabriel and Heiko Maas in 2017. In 2020, she took on the role of Cyber Ambassador in the Department for Global Governance, where the concept for a feminist foreign policy was developed. In 2024, she was appointed Consul General in Istanbul.

Cyber Diplomacy in Singapore and ASEAN

Benjamin Ang and Eugene E.G. Tan

> [Singapore is] O.K. with me, but there are 211 million people [in Indonesia]. Look at that map. All the green [area] is Indonesia. And that red dot is Singapore. Look at that.'[156] (Indonesian President B.J. Habibie, in an interview published in the Asian *Wall Street Journal*, 4 August 1998)

As a small city-state that has always been painfully aware of its diminutive size and corresponding vulnerability, Singapore views diplomacy as an essential part of national strategy. Singapore's approach to diplomacy has been described as 'promoting friendly relations as a way to protect and advance [Singapore's] own important interests',[157] which include a successful and vibrant economy, and peace and stability in the region.[158] This is essential because small states like Singapore lack the economic and military strength to resist pressure from superpowers and large powers (including regional neighbours)

---

[156] Borsuk, R., & Reginald ChuaStaff Reporters. (1998, August 4). *Singapore Strains Relations With Indonesia's President*. The Wall Street Journal. https://www.wsj.com/articles/SB902170180588248000

[157] Full speech: Five core principles of Singapore's foreign policy. (2017, July 17). *The Straits Times*. https://www.straitstimes.com/singapore/five-core-principles-of-singapores-foreign-policy

[158] ibid.

but rely on diplomacy to reduce conflict and increase influence in global decision-making.[159]

One key area of global decision-making that is relevant to small states like Singapore is supporting an international order governed by rule of law and international norms, which upholds the rights and sovereignty of all states.[160] Singapore's diplomacy goals and general foreign policy outlook are largely realist, using multilateral diplomacy in international organisations to exert a disproportionate presence.[161] For example, Singapore has played a leading role in the development of the Law of the Sea Treaty (UNCLOS), participated actively at the World Trade Organization, signed many free trade agreements and participated in the Global Agreement on Climate Change.[162]

---

[159] Gashi, B. (2017). The Role of Small Countries Diplomacy in National, Regional and Global Security Environment. *www.academia.edu*. https://www.academia.edu/79397765/Foreign_Policy_Analysis_The_Role_of_Small_Countries_Diplomacy_in_National_Regional_and_Global_Security_Environment

[160] Full speech: Five core principles of Singapore's foreign policy. (2017, July 17). *The Straits Times*. https://www.straitstimes.com/singapore/five-core-principles-of-singapores-foreign-policy

[161] Eugene E.G. Tan.

[162] ibid.

Singapore and ASEAN prioritise cyber diplomacy

It then comes as no surprise that Singapore prioritises cyber diplomacy. The city state is highly connected and digitalised, and the economy depends heavily on security and stability as a business hub. This makes Singapore vulnerable to transnational cyber threats that move through the region. To mitigate these threats, cyber diplomacy helps build regional cooperation in identifying and responding to them and helps establish international norms of behaviour between states.[163]

The Association of Southeast Asian Nations (ASEAN) member states are aligned with this, having recognised at the 32nd ASEAN Summit in April 2018 that norms and the rule of law are needed for cyberspace, and serve as a basis for using technology to advance economic growth in the region.[164] Singapore was the chair of ASEAN that year.

The ASEAN Summit was followed later that year by the ASEAN Ministerial Conference on Cybersecurity (AMCC), which also agreed that there is a need for a more formalised mechanism

---

[163] Nolan, S. (2022, May 10). *How Singapore is shaping its cyber defence with international collaboration*. GovInsider. https://govinsider.asia/intl-en/article/aixgov-how-singapore-is-shaping-its-cyber-defence-with-international-collaboration-gaurav-keerthi-csa/

[164] Parameswaran, P. (2018, May 2). ASEAN cybersecurity in the spotlight under Singapore's chairmanship. *The Diplomat*. https://thediplomat.com/2018/05/asean-cybersecurity-in-the-spotlight-under-singapores-chairmanship/

for ASEAN cyber coordination, and tasked Singapore to propose a mechanism for the AMCC to consider.[165] The AMCC also agreed in principle to subscribe to the 11 voluntary, non-binding norms of responsible state behaviour recommended by the 2015 UNGGE ('Eleven 2015 UNGGE Norms'), and focus on regional capacity building in implementing these norms.[166] ASEAN was the first regional group to do so.[167]

ASEAN and Singapore's efforts in cyber diplomacy

ASEAN Ministerial Conference on Cybersecurity

Since then, Singapore has continued hosting the annual AMCC at Singapore International Cyber Week (SICW), the flagship annual conference of Singapore's Cybersecurity Agency (CSA) (the national authority for cybersecurity), which is a prominent

---

[165] Eugene E.G. Tan.

[166] Cyber Security Agency of Singapore (CSA). (2024, October 16). *Singapore and ASEAN member states deepen commitment to enhance collective cybersecurity in the region*. CSA Singapore. https://www.csa.gov.sg/News-Events/Press-Releases/2024/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region

[167] *SM Teo Chee Hean at the 6th Singapore International Cyber Week Opening Ceremony:Opening Address by Mr Teo Chee Hean, Senior Minister and Coordinating Minister for National Security, at the 6th Singapore International Cyber Week Opening Ceremony on Tuesday, 5 Oct 2021*. (2021, October 5). Prime Minister's Office Singapore. https://www.pmo.gov.sg/Newsroom/SM-Teo-Chee-Hean-at-the-6th-Singapore-International-Cyber-Week-Opening-Ceremony

regional and international cybersecurity event.[168] AMCC started in 2016 as a platform to bring together ministers and senior officials dealing with cybersecurity issues, and continues to be essential for ASEAN states and partners to dialogue and discuss cybersecurity. This has been no small feat, especially considering that in 2016 most ASEAN states did not have specific ministers in charge of cybersecurity or national agencies responsible for cybersecurity. Singapore's solution was to invite states to send more than one minister until states could resolve the question internally.

In addition to reaffirming the ASEAN leaders' commitment to the Eleven 2015 UNGGE Norms, The continuation of AMCC has led to the creation of the ASEAN regional action plan (RAP) to ensure responsible state behaviour.[169] Singapore's ability to convene regional and extra-regional partners to dialogue, account for their actions and agree on steps forward is an important part of its cyber diplomacy.[170] In 2020, the AMCC committed to develop a long-term regional cybersecurity action plan to implement the norms of responsible state

[168] *About SICW*. (n.d.). The Singapore International Cyber Week (SICW). https://www.sicw.gov.sg/about-sicw/

[169]ASEAN. (2018b, September 27). *Chairman's Statement of The 3rd ASEAN Ministerial Conference on Cybersecurity*. https://asean.org/speechandstatement/chairmans-statement-of-the-3rd-asean-ministerial-conference-on-cybersecurity/

[170] Eugene E.G. Tan.

behaviour in cyberspace, considering the national priorities and cyber capacities of individual ASEAN member states.[171]

Norms implementation checklist

The same year at SICW, Singapore and the UN agreed to develop a checklist to help countries implement norms for responsible state behaviour in cyberspace, based on the Eleven 2015 UNGGE Norms, to guide countries in building a secure and trusted global cyberspace. The checklist builds on ASEAN's previous work to help other countries, especially developing ones, implement these norms by establishing legal frameworks and sharing networks.[172]

The ASEAN–Singapore Cybersecurity Centre of Excellence (ASCCE) has hosted workshops under the UN–Singapore Cyber Programme (UNSCP) to support this effort. The workshops are supported by UNIDIR (UN Institute for Disarmament Research) and involve representatives from ASEAN member states in discussion on how the norms can be operationalised at the national level across the policy, operational, technical, legal and diplomatic domains. UN Under-Secretary-General Izumi

---

[171] *Remarks by Mr S Iswaran, Minister for Communications and Information and Minister-in-charge of Cybersecurity at SICW 2020 Joint Press Conference*. (2020, October 9). CSA Singapore. https://www.csa.gov.sg/News-Events/speeches/2020/sicw-2020-press-conference

[172] Yuen-C, T. (2020, October 9). Singapore, UN to cooperate on checklist for countries to implement cyber-security norms. *The Straits Times*. https://www.straitstimes.com/singapore/politics/singapore-un-to-cooperate-on-checklist-for-countries-to-implement-cybersecurity

Nakamitsu recognised Singapore's leadership in cybersecurity and its key role in fostering a stable and peaceful cyberspace.[173]

In 2024, Singapore's CSA and Malaysia's National Cyber Security Agency (NACSA) finalised the checklist when they co-hosted the ASEAN Norms Implementation Checklist Workshop at the sidelines of the NACSA Cybersecurity Summit in Malaysia. This will allow all ASEAN member states to refer to the document as a practical guide for their next steps and the capacities they will need to build to implement the norms in line with their individual national priorities.[174]

Hopefully this successful act of cyber diplomacy will also be useful to the other states and regional groups participating in discussions at the ongoing UN Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021–2025 as well as regional platforms such as the ASEAN Regional Forum (ARF).

---

[173] Singapore to work with UN to help nations implement norms for responsible cyber behaviour. (2020, November 2). *The Straits Times*. https://www.straitstimes.com/tech/singapore-to-work-with-un-to-help-nations-implement-norms-for-responsible-cyber-behaviour

[174] ASEAN-Singapore Cybersecurity Centre of Excellence. (2024, August 1). *ASEAN-Singapore Cybersecurity Centre of Excellence on LinkedIn: #ascce #cybersecurity #capacitybuilding #asean #unidir*. https://www.linkedin.com/posts/ascce_ascce-cybersecurity-capacitybuilding-activity-7226403223979372546-0lyE/

ASEAN Digital Ministers' Meetings

In addition to the AMCC, Singapore has proposed initiatives to the ASEAN Digital Ministers' Meetings (ADGMINs),[175] including the formation of an ASEAN Data Management Framework (DMF), ASEAN Model Contractual Clauses for Cross Border Data Flows (MCCs) and the proposal to establish an ASEAN CERT (Computer Emergency Response Team) Information Exchange Mechanism for enhancing cybersecurity cooperation.[176] ADGMIN also launched the ASEAN Cybersecurity Cooperation Plan (2021–2025). The ADGMIN Meeting is the forum for ASEAN states to cooperate with partners from all over the world, including China, Korea, Japan, the European Union and the United States.[177]

The ASEAN Data Management Framework and ASEAN MCCs for Cross Border Data Flows initiatives were developed by the ASEAN Working Group on Digital Data Governance, which is chaired by Singapore. These will help businesses in ASEAN

---

[175] The ASEAN Digital Ministers Meeting (ADGMIN) was formerly known as ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), which was first held in July 2001. TELMIN agreed to rename the ministerial body 'ADGMIN' to reflect its expanded scope of work from ICT to digital in October 2019. https://asean.org/our-communities/economic-community/asean-digital-sector/major-sectoral-bodies-committees/

[176] The Ministry of Digital Development and Information (MDDI). (2021, January 22). *1st ASEAN Digital Ministers' Meeting approves Singapore led initiatives* [Press release]. https://www.mddi.gov.sg/media-centre/press-releases/1st-asean-digital-ministers-meeting-approves-singapore-led-initiatives/

[177] Eugene E.G. Tan.

implement data management, including guidelines for data governance structures and data protection safeguards, as well as harmonise contractual terms among ASEAN countries for transferring personal data to each other across borders.[178]

The ASEAN Digital Masterplan 2025 envisions the ASEAN region becoming both a digital economy and a digital society, much like Singapore aims to become through its Smart Nation vision.[179]

The 2nd ADGMIN Meeting held in 2022 launched the ASEAN Cybersecurity Cooperation Strategy (2021–2025) to enhance regional cybersecurity cooperation and address the evolving cyber-threat landscape.[180] Its objectives include advancing cyber cooperation, strengthening coordination for cyber policy to create a unified approach, enhancing trust in cyberspace among ASEAN member states, regional capacity building, and engaging with international partners.

---

[178] ASEAN. (2023). The 3rd ASEAN Digital Ministers' Meeting and Related Meetings Boracay, Malay, Aklan, Philippines, 9-10 February 2023. In *ASEAN*. https://asean.org/wp-content/uploads/2023/02/Endorsed-3rd-ADGMIN-JMS.pdf

[179] ASEAN. (2021, January 22). *Joint Media Statement of The 1st ASEAN Digital Ministers' Meeting and Related Meetings* [Press release]. https://asean.org/joint-media-statement-of-the-1st-asean-digital-ministers-meeting-and-related-meetings/

[180] Bin Abdul Rahman, M. (2023, January 4). *Advancing Cyber And Information Security Cooperation In ASEAN – Analysis*. Eurasiareview. https://www.eurasiareview.com/04012023-advancing-cyber-and-information-security-cooperation-in-asean-analysis/#google_vignette

The 3rd ADGMIN Meeting held in 2023 endorsed the creation of an ASEAN Regional CERT Operational Framework to help allocate resources required for the implementation of the ASEAN Regional CERT and further guide CERT-related capacity-building efforts through regional cybersecurity capacity-building programmes conducted by the ASCCE and the ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC).[181]

Regional capacity building and ASCCE

ASCCE, which is managed by CSA and located in Singapore, has been actively building technical, policy, and legal capacity among ASEAN member states. Its work includes conducting research; training in international law, cyber strategy, legislation, cyber norms and other cybersecurity policy issues; CERT-related technical training; facilitating exchange of open-source cyber threat and attack-related information and best practices; and conducting virtual cyber defence training and exercises.[182] This helps to provide ASEAN states with the expertise to tackle cyber breaches.[183]

---

[181] ASEAN. (2023). The 3rd ASEAN Digital Ministers' Meeting and Related Meetings Boracay, Malay, Aklan, Philippines, 9-10 February 2023. In *ASEAN*. https://asean.org/wp-content/uploads/2023/02/Endorsed-3rd-ADGMIN-JMS.pdf

[182] CSA Singapore. (2021, October 6). *ASEAN-Singapore Cybersecurity Centre of Excellence*. https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence

[183] Eugene E.G. Tan.

ASCCE also hosts the UN–Singapore Cyber Fellowship Programme, which was jointly launched by the National University of Singapore, ASCCE and the United Nations Office for Disarmament (UNODA), in September 2022.[184] Since then, it has been running twice yearly and has brought scores of diplomats and senior cybersecurity leaders from UN member states to ASCCE to learn cyber and digital security policymaking, strategies and operations, as well as to build relations and network, making it significant not only for capacity building but also as a confidence-building measure.

At SICW 2023, Singapore's deputy prime minister, Heng Swee Kiat, announced the launch of the SG Cyber Leadership and Alumni Programme under ASCCE, and that Singapore would extend its funding commitment of S$30 million for cyber capacity building to 2026. The programme includes training courses at different levels, open to all countries, covering cyber diplomacy, international law, norms in cyberspace and cyber-threat mitigation strategies, and provides officials involved in multilateral cyber discussions with operational and technical cyber policy knowledge.[185]

---

[184] National University of Singapore. (2022, September 13). *NUS jointly launches inaugural UN-Singapore Cyber Fellowship Programme*. NUS News. https://news.nus.edu.sg/nus-jointly-launches-inaugural-un-singapore-cyber-fellowship-programme/

[185] *Singapore Deepens Commitment to a Secure Cyberspace Through Capacity Building*. (2023, October 17). CSA Singapore. https://www.csa.gov.sg/News-Events/Press-Releases/2023/singapore-deepens-commitment-to-a-secure-cyberspace-through-capacity-building

ADMM Cyber and Information Centre of Excellence

The defence sector of ASEAN also has a role to play in cyber diplomacy. The ASEAN Defence Ministers' Meeting (ADMM) set up the ADMM Cybersecurity and Information Centre of Excellence (ACICE), among other reasons, to enhance multilateral cooperation among ASEAN defence establishments to combat cyberattacks, disinformation and misinformation, as well as capacity building and information sharing. The centre is managed and located in Singapore by the Ministry of Defence.[186]

ACICE's flagship event and key confidence-building measure is the annual Digital Defence Symposium (DDS) in Singapore, which provides a platform for ASEAN and international cyber defence officials and experts to discuss strategies, collaboration and cooperation.[187]

---

[186] MINDEF Singapore. (2023, July 18). *Minister's Speech at the ADMM Cybersecurity and Information Centre of Excellence (ACICE) Official Opening Ceremony on 18 July 2023*. https://www.mindef.gov.sg/news-and-events/latest-releases/18jul23_speech

[187] *ASEAN and international defence experts address cyber and information threats at Digital Defence Symposium | Indiplomacy*. (2024, July 25). https://indiplomacy.com/2024/07/25/asean-and-international-defence-experts-address-cyber-and-information-threats-at-digital-defence-symposium/

Bilateral Memorandums of Understanding

Singapore has signed cybersecurity Memorandums of Understanding (MOUs) with several countries, including the United States, Canada, Australia, India, Qatar and others. These usually include regular exchanges of information on cyber threats, coordination of response to cybersecurity incidents, and joint cybersecurity training and exercises.

United Nations processes

Singapore has been supportive of continuing discussions at the United Nations, voting to advance both the UN OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security and the UNGGE in 2018, and the creation of a new OEWG (for 2021 to 2025) in 2020.[188]

The chief executive of Singapore's Cyber Security Agency, David Koh, chaired the intersessional multistakeholder meeting, from 2 to 4 December 2019, of the first OEWG. The Global Commission on the Stability of Cyberspace credited this for providing 'a stage to illustrate the contributions that non-

[188] *First committee approves 27 texts, including 2 proposing new groups to develop rules for states on responsible cyberspace conduct*. (2018, November 8). UN Meetings Coverage and Press Releases. https://www.un.org/press/en/2018/gadis3619.doc.htm

governmental actors were able to make'.[189] The Commission praised the OEWG's adoption of its final report by consensus on 12 March 2021 as 'a milestone for institutional dialogues on international peace and security in cyberspace'.[190]

For the subsequent OEWG (2021–2025), Singapore's Permanent Representative to the UN, Ambassador Burhan Gafoor, was elected as chair.[191] He has the unenviable task of presiding over a process under pressure from immense geopolitical turmoil including the Russian invasion of Ukraine and great power competition between the US and China. Amid these challenges, he has been described as 'able and indefatigable' and constantly seeking to 'identify points of convergence en route to "concrete results" in this wide-ranging exchange of views'.[192] The chair has managed with skilled diplomacy to build enough consensus to produce annual progress reports so far, often after many rounds of discussions,

---

[189] *UN Open-Ended Working Group adopts final report by consensus*. (2021, March 21). HCSS. https://hcss.nl/news/un-open-ended-working-group-adopts-final-report-by-consensus/

[190] ibid.

[191] *SM Teo Chee Hean at the 6th Singapore International Cyber Week Opening Ceremony: Opening Address by Mr Teo Chee Hean, Senior Minister and Coordinating Minister for National Security, at the 6th Singapore International Cyber Week Opening Ceremony on Tuesday, 5 Oct 2021*. (2021, October 5). Prime Minister's Office Singapore. https://www.pmo.gov.sg/Newsroom/SM-Teo-Chee-Hean-at-the-6th-Singapore-International-Cyber-Week-Opening-Ceremony

[192] ICT4Peace. (2023, March 15). *UN OEWG – The plot thickens: The UN Open-Ended Working Group on ICTs – Fourth session – ICT4Peace Foundation*. https://ict4peace.org/activities/un-oewg-the-plot-thickens-the-un-open-ended-working-group-on-icts-fourth-session/

and sometimes with states disassociating themselves, as Iran did in 2021.[193]

Challenges faced by Singapore and ASEAN in cyber diplomacy

Geopolitical tensions and the OEWG

Despite the best efforts of the chair of the OEWG (2021–2025), the meeting faces formidable geopolitical challenges. While Singapore has been described as 'punching above its weight' in global governance,[194] the geopolitical tensions of the 2020s are heavyweight. The East–West divide, between Western countries (US and Europe) on one hand and Russia and China on the other, has grown even wider since the Russian invasion of Ukraine. Consequently, states on opposing sides are unable or unwilling to resolve the long-standing disagreements on key cyber issues (such as whether a legally binding treaty is needed) and unwilling to agree on newer key issues (such as the form

[193] Council on Foreign Relations (CFR). (2021, March 18). Unexpectedly, all UN countries agreed on a cybersecurity report. So what? *Council on Foreign Relations*. https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what

[194] Global-Is-Asian. (2018, August 1). *Punching Above Its Weight: Is Singapore More Than A Price Taker in Global Governance?* https://lkyspp.nus.edu.sg/gia/article/punching-above-its-weight-is-singapore-more-than-a-price-taker-in-global-governance

of future institutional dialogue after the OEWG ends in 2025).[195] The chair has had to intervene several times during the substantive meetings to keep member states focused on the cyber discussions at hand, instead of letting them side-track into condemnation and counter-condemnation over the war. Consensus is extremely difficult to build under these conditions. As the process comes to the close in 2025, the future of regular institutional dialogue is still up in the air.

Great power competition between US and China

ASEAN member states have resisted being drawn into major power competition for many reasons, including economic ties to and dependence on both major powers and the risks to regional stability. Keeping in mind that the United States' current International Cyberspace & Digital Policy Strategy describes China as its largest cyber threat,[196] this makes cyber diplomacy essential in balancing ASEAN member states' relationships with both powers. Experts cite the risk that cyber conflict between the major powers could spill into the ASEAN

[195] Hurel, L. (2022, September 6). The rocky road to cyber norms at the United Nations. *Council on Foreign Relations*. https://www.cfr.org/blog/rocky-road-cyber-norms-united-nations-0
[196] *United States International Cyberspace & Digital Policy Strategy - United States Department of State*. (2024, May 6). United States Department of State. https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/

region and recommend that ASEAN promote cyber norms to mitigate this.[197]

Singapore in particular needs to balance its security partnership with the US and its trading relationship with China. While the US regional presence is essential to regional security, China is Singapore's most important trading partner.[198] On one hand, Singapore is a key security partner for the US because of logistics access and infrastructure for US maritime and air forces and security assistance programmes.[199] On the other hand, in 2022, China's exports to Singapore grew to USD 73.3bn (largest sectors were refined petroleum, integrated circuits and broadcasting equipment) and Singapore exported USD 51.2bn to China.[200]

Differences in cyber maturity in the region

Cyber diplomacy in ASEAN has taken a serious investment of Singapore's resources in capacity building, such as the S$30 million (USD 23.4 million) fund mentioned above. This is

---

[197] Rahman, M. F. A. (2024, May 14). ASEAN should watch the China-US cyber competition more closely. *The Diplomat*. https://thediplomat.com/2024/05/asean-should-watch-the-china-us-cyber-competition-more-closely/

[198] Cooper, C. A., & Chase, M. S. (2020). *Regional responses to U. S. - China competition in the Indo-Pacific: Singapore*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR4400/RR4412z5/RAND_RR4412z5.pdf

[199] ibid.

[200] *China (CHN) and Singapore (SGP) trade*. (2024, November). *The Observatory of Economic Complexity (OEC)*. https://oec.world/en/profile/bilateral-country/chn/partner/sgp

because ASEAN member states vary widely in their cyber maturity and digital integration. At one end of the spectrum, Singapore and Malaysia are recognised for their national cybersecurity strategies, agencies and infrastructure. At the other end, Myanmar, Cambodia[201] and Laos[202] (the chair of ASEAN for 2024) lack resources, infrastructure and a skilled cyber workforce.

Future steps for Singapore and ASEAN

Singapore has leveraged its strategic position and cyber maturity to drive cyber diplomacy by leading regional initiatives, international collaboration and capacity building. In the coming years, we are likely to see continued dialogue and cooperation in bilateral dialogues like the United States–Singapore Cyber Dialogue (USSCD)[203] and in multinational and regional fora.

---

[201] Corrado, R., & Sakal, M. (2021). Cybersecurity in Cambodia: Awareness as a first step. In CD-Center, *CD-Center* (Vols. 3–3, Issue 11, pp. 2–8). https://cd-center.org/wp-content/uploads/2021/08/P124_20210805_V3IS11_EN.pdf

[202] International Bank for Reconstruction and Development / The World Bank. (2022). *Positioning The LAO PDR For A Digital Future: Priority Measures To Accelerate Digital Economy Development: Priority Measures To Accelerate Digital Economy Development*. https://documents1.worldbank.org/curated/en/099445010192229771/pdf/P177067071faad02c0b7ec0ec39157cfae9.pdf

[203] *The Inaugural U.S.-Singapore Cyber Dialogue - United States Department of State*. (2022, November 3). United States Department of State. https://www.state.gov/the-inaugural-u-s-singapore-cyber-dialogue/

Public–private partnership is another aspect of cyber diplomacy that is essential, because the private sector not only owns and operates most of the critical infrastructure but also provides cybersecurity protection for most organisations. This is most evident in Microsoft's role in defending Ukraine against cyberattacks from Russia. Most recently, CSA signed an MOU with global cybersecurity company Dragos, Inc., covering information-sharing and capacity and capability building for Operational Technology (OT) cybersecurity.[204]

Singapore also has an opportunity to convene dialogue between the major powers in cyber, building on efforts like the 5th RSIS Trilateral Exchange forum, which the S. Rajaratnam School of International Studies (RSIS) hosted in April 2024, where scholars from China and the US met in Singapore.[205] Cyber conflict was not expressly discussed during that forum, but experts suggest it could be on the agenda in future meetings.[206] One participant made the interesting observation that even during the Cold War, despite deep mistrust between

---

[204] CSA Singapore. (2023, August 22). *CSA and Dragos, Inc. Sign Memorandum of Understanding to Strengthen Singapore's Capabilities in Operational Technology Cybersecurity* [Press release]. https://www.csa.gov.sg/News-Events/Press-Releases/2023/csa-and-dragos-inc-sign-memorandum-of-understanding-to-strength-singapore-s-capabilities-in-operational-technology-cybersecurity

[205] *5th RSIS Trilateral Exchange Rising to the Challenge: Global Leadership in a Fractured World*. (2024, April 25). RSiS. https://www.rsis.edu.sg/event/5th-rsis-trilateral-exchange/

[206] Rahman, M. F. A. (2024, May 14). ASEAN should watch the China-US cyber competition more closely. *The Diplomat*. https://thediplomat.com/2024/05/asean-should-watch-the-china-us-cyber-competition-more-closely/

the US and the Soviet Union, they were able to agree on issues such as nuclear controls and, most importantly, avoided direct conflict.[207] Hopefully this can apply to cyber as well.

In any event, Singapore has no option but to pursue cyber diplomacy. Ambassador Burhan Gafoor has put it well:

As a small state, Singapore has always supported a rules-based multilateral system rooted in respect for international law. Our approach is no different regarding cyberspace. To maintain a cyberspace that is secure, trusted, open, and interoperable, we must adopt a global approach, based on global rules and norms and adherence to international law. To do so will be challenging, given the backdrop of a volatile and fractious global landscape caused by growing geopolitical tensions. However, we have no option but to continue to advocate and support the applicability of international law and norms in order to encourage responsible state behaviour in cyberspace. We need to double down on international collaboration for greater cyber resilience and stability. (Ambassador Burhan Gafoor), Permanent Representative of the Republic of Singapore, at the UN Security Council Open.

[207] Kwang, H. F. (2024, April 29). Commentary: What to do when the US-China rivalry gulf remains deep, wide and long-lasting. *CNA*. https://www.channelnewsasia.com/commentary/china-us-ties-tension-diplomatic-meetings-gulf-deep-wide-long-lasting-4298141

Mr Benjamin Ang

Head of Centre of Excellence for National Security (CENS), Future Issues in Technology (FIT), Digital Impact S. Rajaratnam School of International Studies (RSIS)

Benjamin Ang is Head of the Centre of Excellence for National Security (CENS), Future Issues in Technology, and Digital Impact Research, at RSIS. He leads the policy research think tank that focuses on national security aspects of Cyber, Hybrid Threats, Disinformation, Foreign Interference, Extremism, Emerging Technologies, AI, Quantum, Space, Biotech, Energy, and Smart Cities. Before his academic career, Benjamin was a lawyer, network sysadmin, CIO (chief information officer), technology consultant, and educator. Since joining CENS, he has testified before the Select Committee on Online Falsehoods, spoken at the United Nations Open Ended Working Group on Cyber, and contributed to numerous lectures and training programmes including the UN Singapore Cyber Programme and the UN Cyber Diplomacy course.

Mr Eugene EG Tan

Associate Research Fellow, S. Rajaratnam School of International Studies (RSIS)

Eugene Tan is an Associate Research Fellow specialising in cyberspace security issues, Singapore's foreign policy, and aviation issues. Eugene holds a Masters of International Studies and a Postgraduate Diploma in Arts (Politics) from the University

of Otago, and a Bachelor of Arts from the National University of Singapore.

Part 4

KEY FUNCTIONAL TOPICS

United Nations Negotiations on Information and Communication Technology in the Context of International Security

Karsten Geier

A new technology

Shortly before the turn from the nineteenth to the twentieth century, in the outskirts of Berlin, a man drew crowds with a strange spectacle: he would carry a contraption made of wood, wire and cotton up a hill, somehow clamber into it, run downhill, then suddenly jump in the air and—fly. This man's name was Otto Lilienthal. He built the world's first heavier-than-air gliders. A few years later, Americans Wilbur and Orville Wright mounted a combustion engine onto a machine constructed according to Lilienthal's principles, making it possible to take off from even ground and sometimes even return to Earth unharmed. (In initially rare cases, the flying machine could be used a second time.)

This invention sparked a host of questions. Who owned the airspace through which aircraft flew? Which rules applied? If these machines could cross borders and ground-based

defences without control, what did that mean for international peace and security? This last issue was particularly vexing. In 1911, at a meeting of the renowned Geneva Institute of International Law, legislation was proposed simply to ban the use of airplanes as platforms for weapons. It did not pass.

130 years after Lilienthal's ground-breaking (or rather ground-leaving) exploits, almost the same questions have arisen with respect to another technological breakthrough: information and communication technology (ICT). Who owns cyberspace? Which rules apply? What does the use of ICT by states mean for international peace and security? Once more, there are calls to ban the use of a new technology for military purposes—while ICT already has become an instrument of international conflict. The most prominent forum for these discussions is the United Nations.

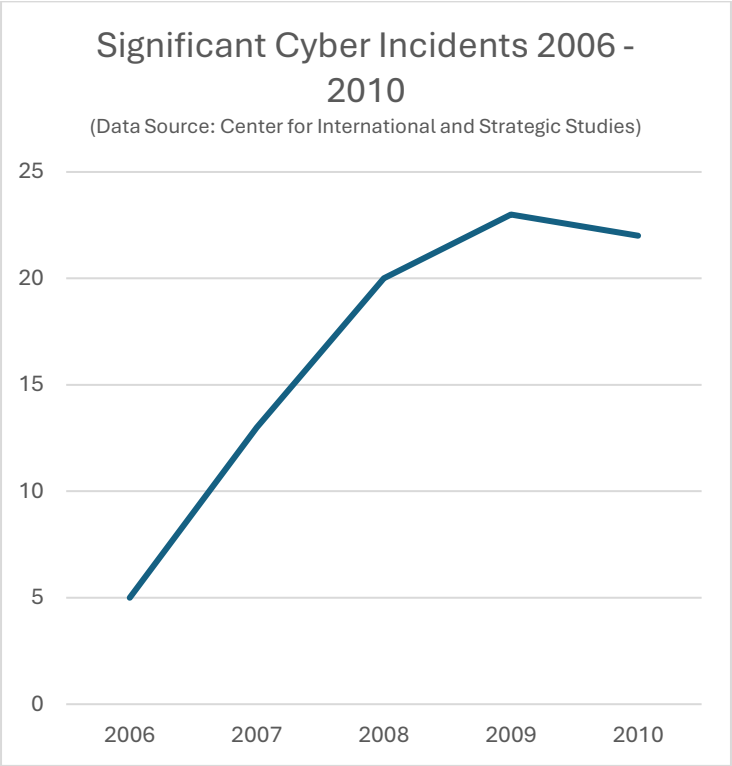
The issue was first raised in the late 1990s by Russian diplomats, worried about 'information security'. They met with scepticism—this was a time when a computer stood on a desk, linked via telephone modem to the nascent internet. Electronic communication was so innovative and rare that Hollywood made a movie called 'You 've got mail', in which Meg Ryan was waiting impatiently for her mailbox to pop up a message from co-starring Tom Hanks. What implications could the stuff of romantic comedies possibly have for international peace and security?

The Russians persisted, and in 2004 convinced the UN General Assembly to request the Secretary-General *to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, and to conduct*

a study … with the assistance of a group of governmental experts (GGE).[208] The experts did not reach a consensus, and hence had no advice for the Secretary-General.

In 2009/2010, another GGE was convened. After difficult negotiations, this group did present a paper. The authors argued that *existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century*.[209]

[208] Paragraph 4, *Resolution on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/RES/58/32, 18 December 2003. http://www.worldlii.org/int/other/UNGA/2003/77.pdf
[209] Paragraph 1, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/65/201, 30 July 2010. https://digitallibrary.un.org/record/688507?ln=en&v=pdf



Six years' time difference, similar setup (even the same chair, Russian cyber ambassador Andrey Krutskikh)—yet radically different outcomes. This not only bears witness to the diplomatic skill of the experts involved, but also reflects the fact that in the meantime, ICT had gained visibility, importance—and disruptive potential. Shortly before the first GGE was convened, in December 2003, the World Summit on the Information Society could still formulate an idealistic vision of a *people-centered, inclusive and development-oriented*

Information Society, in which ICT would promote *the attainment of a more peaceful, just, and prosperous world*.[210] By 2010, Blackberries and iPhones had brought the internet into users' palms, and IT-based supervisory control and data acquisition systems for machines were producing an industrial revolution. All this created new targets as well as multiplying attack surfaces, and the number of cyber operations rose. The *information society* of pink ponies and sparkling rainbows was in retreat: it is no coincidence that Washington's Center for Strategic and International Studies begins its list of significant cyber incidents in 2006.[211] No longer the stuff of romantic comedies, ICT incidents gained political importance: in 2007, Estonian government networks were disrupted by a denial-of-service attack; some online services and online banking were halted. In October 2010, shortly after the GGE had spoken of *one of the most serious challenges of the twenty-first century*, a complex piece of malware designed to interfere with the industrial control systems of centrifuges used in Iran's nuclear programme was discovered. ICT had arrived in the heart of international security.

There has since been an almost exponential growth in ICT operations targeting both private and public IT systems. Cyber

---

[210] International Telecommunication Union (ITU). (2003, December 12). *World Summit on the Information Society Declaration of Principles', Document WSIS-03/GENEVA/DOC/4-E*. https://www.itu.int/net/wsis/docs/geneva/official/dop.html

[211] Center for Strategic and International Studies (CSIS). (n.d.). *Significant Cyber Incidents Since 2006*. CSIS. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

has become a military domain. Roughly half the world's countries are known to hold military ICT capabilities. In conflict theatres from Ukraine to the Middle East and Africa, ICT operations are accompanying kinetic battlefield action.

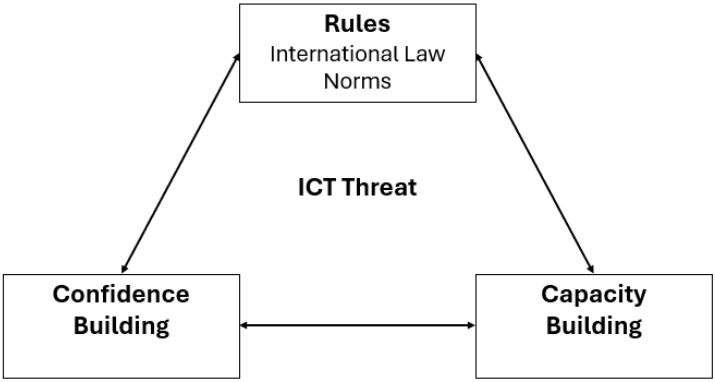
Most ICT incidents are technical in nature—they are mishaps. Some have a criminal background. Only the smallest part is connected to political or even military objectives. The damage those do, however, is beyond estimate—and it is often damage to non-conflicting parties. The Russian war of aggression against Ukraine is illustrative: between January 2022 and September 2023, the Geneva-based Cyber Peace Institute observed 574 ICT attacks and operations directed at Ukraine, but 1,896 such operations targeting non-belligerent third countries (Poland, Lithuania, Germany, the United States and Estonia held the top five slots).[212]

Risks are not limited to the technical sector: in an era of 'unpeace' and hybrid warfare, ICT-enabled social media campaigns have turned into a powerful instrument to influence political debates and decision-making. Technological developments are reinforcing these trends: Artificial Intelligence (AI) facilitates coding for ICT operations; generative AI allows production of false or misleading information at an unprecedented depth, scale and scope for (ab)use in political influence campaigns. New disruptive technologies are looming on the horizon: quantum computing will make even the best-

[212] CyberPeace Institute. (2023). *Cyber dimensions of the armed conflict in Ukraine*. https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf

protected data sets vulnerable. Brain–machine interfacing may open heretofore unexplored attack vectors.

Responding to the 2010 GGE warning about ICT threats to peace and security, the UN has made considerable progress in addressing these challenges. A triangle of responses has emerged. The corners of this triangle are (1) rules of responsible state behaviour, (2) building confidence that states will respect these rules, and (3) helping those lacking capacity to behave in a rule-abiding and confidence-inspiring way.



International law

A key step forward was agreement that *international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.* This was

first formulated in the 2013 GGE report,[213] of which the General Assembly took note in 2014[214] before explicitly welcoming it two years later.[215]

Another GGE report in 2015 noted *the inherent right of States to take measures consistent with international law and as recognized in the (UN) Charter*[216] and identified *as of central importance the commitments of States to … sovereign equality; the settlement of international disputes by peaceful means…; refraining … from the threat or use of force…; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States*.[217]

---

[213] Paragraph 19, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* UN document A/68/98, 24 June 2013. https://documents.un.org/doc/undoc/gen/n13/371/66/pdf/n1337166.pdf. The United Nations General Assembly took note of (i.e. cautiously approved) the report on 9 January 2014 in Resolution A/RES/68/243. Two years later, in a preambular paragraph to its Resolution A/RES/70/237 of 30 December 2015, the General Assembly went a step further and explicitly welcomed the conclusion on the applicability of international law.

[214] Resolution A/RES/68/243, 9 January 2014. https://ccdcoe.org/uploads/2018/11/UN-131227-ITIS.pdf

[215] Resolution A/RES/70/237, 30 December 2015. https://documents.un.org/doc/undoc/gen/n15/457/57/pdf/n1545757.pdf

[216] Paragraph 28c, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* UN document A/70/174, 22 July 2015. https://digitallibrary.un.org/record/799853?ln=en&v=pdf

[217] ibid., paragraph 26.

Yet another such group in 2016–2017 discussed hotly how to put some meat on these bare bones but could not agree on a consensus report. Finally, in 2021, yet another GGE, once more *noting the inherent right of States to take measures consistent with international law and as recognized in the (UN) Charter*, also mentioned *the principles of humanitarian law (humanity, necessity, proportionality and distinction*). These formulations imply (without saying explicitly) that the law of armed conflict (both the *ius ad bellum* and the *ius in bello*) applies to the use of ICT by states. The GGE recommended *further sharing and exchanging of views … on how international law applies*.[218]

In 2023, the UN Secretary-General summarised that *the information and communications technologies environment is not a lawless space. The rule of law exists in the digital sphere just as it does in the physical world… (This) progress has been hard won and must serve as a baseline for all future multilateral work in this area*.[219]

---

[218] Paragraph 95, recommendation b, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN document A/76/135, 24 July 2021. https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf; The United Nations General Assembly, in its resolution A/RES/67/19 of 8 December 2021, welcomed the 2021 GGE report and called upon member states to be guided by it in their use of ICT. It has since repeated and slightly widened this appeal in its Resolution A/RES/77/37 of 12 December 2022.

[219] Paragraph 42, *Report of the Secretary-General on a Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of*

The emerging consensus on the application of binding international law to state use of ICT has not kept some countries—notably Russia, supported by Belarus, Cuba, Nicaragua, North Korea, Syria and Venezuela—from calling for a treaty to regulate 'international information security'.[220] While Burundi, China, Eritrea, Iran and Zimbabwe are among those on record as supporting this proposal,[221] it is meeting with vehement opposition from the United States and its allies, as well as many other rule-of law-oriented and democratic countries.[222]

International Security, UN document A/78/76, 18 April 2023. https://documents.un.org/doc/undoc/gen/n23/110/82/pdf/n2311082.pdf

[220] 'Updated Concept of the Convention of the United Nations on Ensuring International Information Security', submitted as a working paper to the United Nations' Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies, 29 June 2023. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf

[221] See 'Compendium of Statements in Explanation of Position on the Adoption of the Progress Report of the Open-ended Working Group as Contained in A/79/214', UN document A/AC.292/2024/INF/5, 3 September 2024. https://documents.un.org/doc/undoc/gen/n24/217/49/pdf/n2421749.pdf

[222] For an in-depth analysis, see Valentin Weber's 21 March 2023 blog post for the Council on Foreign Relations: https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security

Norms of responsible state behaviour

In addition to exploring the application of binding international law to state use of ICT, GGE experts have formulated something else: non-binding peacetime norms, rules, and principles for the responsible behaviour of states. The 2015 GGE report elaborated 11 such norms, explaining that *voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. [They] do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States.*[223]

The 2015 ICT norms cover the following elements:

a. Cooperation on stability and security in the use of ICT and on preventing harmful practices
b. Careful responses in case of ICT incidents (States should consider all relevant information)
c. The use of states territory for internationally wrongful acts using ICT
d. Information, exchange on terrorist and criminal use of ICT
e. Respect for Human Rights on the internet

---

[223] Paragraph 13, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/70/174, 22 July 2015.
https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf

f. ICT activity contrary to international law that damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public
g. Protection of critical infrastructure from ICT threats
h. Requests for assistance in case of attacks on critical infrastructure
i. The integrity of the ICT supply chain
j. Responsible reporting of ICT vulnerabilities and sharing available remedies
k. The role of computer emergency response teams.

An important part of discussions in the 2016–2017 and 2020–2021 GGEs was fleshing out these norms. The 2021 GGE report offered useful guidance,[224] and how to implement the 'cyber norms' continues to be under discussion.

Although the 2015 GGE report suggested that *additional norms could be developed over time*,[225] no such consensus has been found.

---

[224] Paragraphs 15–68, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN document A/76/135, 14 July 2021. https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf

[225] Paragraph 15, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/70/174, 22 July 2015. https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf

The compliance problem

The abovementioned series of UN expert groups, two OEWGs and a body of scientific research[226] have established a widely shared set of understandings regarding the rules concerning state use of ICT—both binding international law and non-binding norms of behaviour. However, reality is showing that these do not sufficiently constrain all states' behaviour. International law and norms assume that all states desire to preserve international peace and security. Unfortunately, there are a few for whom this assumption does not hold. The problem is not the absence of agreed rules and measures—it is the lack of a mechanism to promote compliance. This is closely linked to attribution: as long as perpetrators can hide or plausibly deny their actions, rule compliance will remain deficient. Improving attribution has hence been raised repeatedly in the United Nations, but proposals for some sort of UN mechanism to this end have led nowhere.

Individual governments regularly 'call out' governments that they have found violating rules of responsible use of ICT and have even initiated national legal proceedings against those they assume to be responsible. Joint responses by several governments are the exception. In one unusual case of collective attribution, the European Union gathered, on 10 May 2022, a number of international partners to condemn jointly

[226] Note in this context that Art. 38 of the Statutes of the International Court of Justice recognises the *teachings of the most highly qualified publicists of the various nations, as (a) subsidiary means for the determination of rules of law*.

malicious cyber activity conducted by the Russian Federation against Ukraine (which, in the event, targeted the satellite KA-SAT network, owned by USA-based Viasat, and did extensive damage not only in Ukraine but also in the EU). They spoke of an *unacceptable cyberattack that constituted yet another example of Russia's continued pattern of irresponsible behaviour in cyberspace, contrary to the expectations set by all UN Member States, of responsible State behaviour*.[227]

Attributing ICT incidents to a foreign government poses significant challenges. There is no clarity as to who holds precisely which capacities. Some of the most important ICT capabilities are not even in the hands of governments, and although *States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs,*[228] *the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State*.[229] There is an unknown number of private actors that may

---

[227] Council of the EU. (2022, May 10). *Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

[228] Paragraph 13 c, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/70/174, 22 July 2015. https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf

[229] ibid, Paragraph 28 f.

or may not be acting on behalf of or even under the control of a central authority. Decision-making mechanisms, roles and responsibilities can hence be difficult to establish.

Wrongful attribution carries its own risks. It may lead to a hostile response and further escalation. Suppose there is a cyber operation using the ICT infrastructure of a particular country, of which the government is not even aware. Many governments fear they may be censured or even punished for such incidents, although there was nothing they could have done to intervene. Such risks of misattribution and wrongful response need to be controlled.

These considerations have incited UN experts to produce guidance on the attribution of ICT incidents: paragraph 13b of the 2015 GGE report warned that in *case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences*.[230]

The 2021 GGE report elaborated:

A State that is victim of a malicious ICT incident should consider all aspects in its assessment of the incident. Such aspects, supported by substantiated facts, can include the incident's technical attributes; its scope, scale and impact; the wider context, including the incident's bearing on international peace and security; and the results of consultations between the States concerned … (To) facilitate the investigation and resolution of ICT incidents involving other States, States can

[230] ibid.

establish or strengthen relevant national structures, ICT-related policies, processes, legislative frameworks, coordination mechanisms, as well as partnerships and other forms of engagement with relevant stakeholders to assess the severity and replicability of an ICT incident. Furthermore: Cooperation at the regional and international levels … can strengthen the ability of States to detect and investigate malicious ICT incidents and to substantiate their concerns and findings before reaching a conclusion on an incident.[231]

Confidence building

With a view to promoting rule-abiding behaviour rather than responding to rule violations, UN experts have developed cyber confidence-building measures. The 2010 GGE report recommended confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict.[232] Subsequent GGEs took this up, and the 2015 report

[231] Paragraphs 22 ff., *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN document A/76/135, 24 July 2021. https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf

[232] Paragraph 18 (ii), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/65/201, 30 July 2010. https://digitallibrary.un.org/record/3964709/files/DSS_33.pdf

in particular made progress on this issue. Experts suggested, inter alia:

- Points of contact at the policy and technical levels
- Bilateral, regional, subregional and multilateral confidence-building
- Voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICT (vulnerabilities and identified harmful hidden functions in ICT products; best practices for ICT security; national organisations, strategies, policies and programmes relevant to ICT security; etc.)
- Voluntary provision of states' views of categories of infrastructure that they consider critical
- A repository of national laws and policies for the protection of data and ICT-enabled infrastructure
- Mechanisms to address ICT-related requests.[233]

The 2021 GGE report elaborated on points of contact as well as dialogue and consultations. However, in the intervening period it had become clear that most ICT confidence building was taken forward in regional contexts, with the Organization for Security and Co-operation in Europe,[234] the Association of

[233] Paragraph 16, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/70/174, 22 July 2015. https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf

[234] See 'OSCE Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies', PC. Dec/1202, 10 March 2016,

Southeast Asian Nations Regional Forum,[235] the African Union[236] and the Organization of American States[237] leading the way. Only with the establishment of two OEWGs on Developments in the Field of Information and Telecommunications in the Context of International Security (2019–2021 and 2021–2025) did ICT confidence building come again to the forefront of UN work.[238] One concrete outcome is the development of a Global Directory of Cyber Points of

[235] See 'ASEAN Regional Forum Work Plan on Security in and of the Use of Information and Communication Technologies', 7 May 2015.
[236] See African Union Convention on Cyber Security and Personal Data Protection, 27 June 2014.
[237] Under the auspices of the Inter-American Committee against Terrorism.
[238] Paragraphs 41–53, *Final Substantive Report*, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/AC.290/2021/CRP.2, 10 March 2021. https://dig.watch/wp-content/uploads/2022/08/OEWG-Report.pdf ; paragraph 16, *First Annual Progress Report,* Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025', UN document A/77/275, 8 August 2022. https://documents.un.org/doc/undoc/gen/n22/454/03/pdf/n2245403.pdf ; paragraphs 37–42, *Second Annual Progress Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, UN document A/78/265, 1 August 2023. https://documents.un.org/doc/undoc/ltd/n23/227/59/pdf/n2322759.pdf ; and paragraphs 42–49 of the *Third Annual Progress Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, UN document A/79/214, 22 July 2024. https://documents.un.org/doc/undoc/gen/n24/217/49/pdf/n2421749.pdf

Contact.[239] Another, less-noted element of ICT confidence building is member states' efforts to increase transparency through voluntary reporting and information-sharing. Since 1998, the UN Secretary-General has been reporting annually on the views of UN member states concerning ICT in the context of international security.

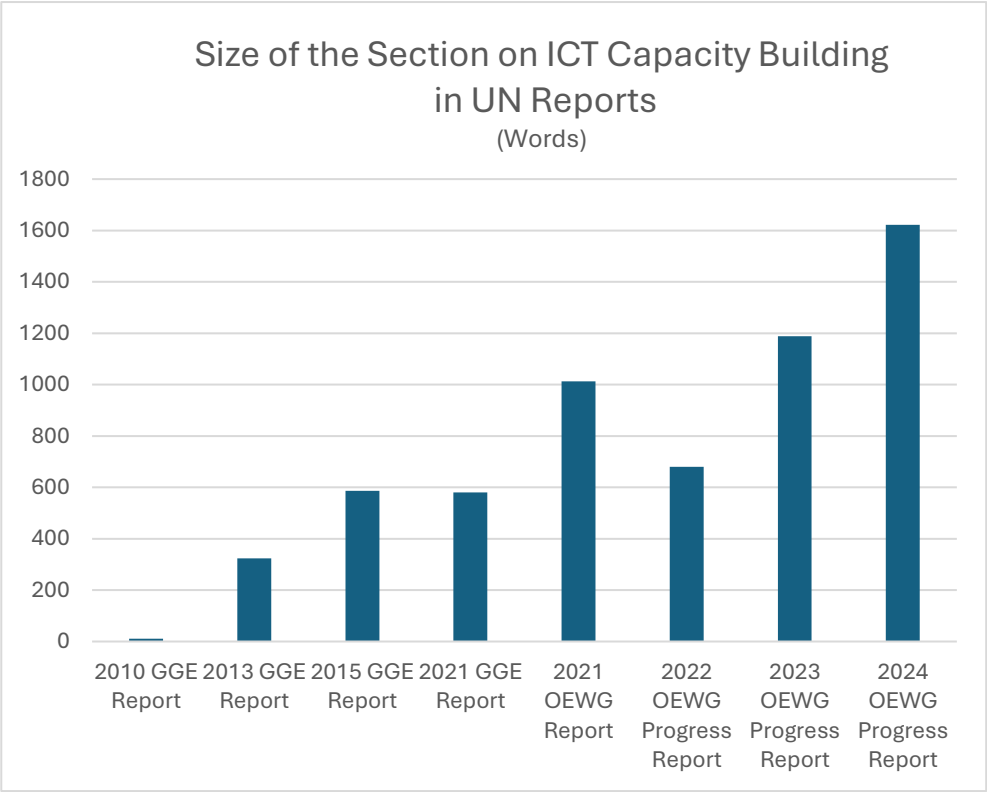
Capacity building

Cyber capacity building was brought into negotiations on ICT in the context of international peace and security with the argument that while all states are vulnerable to ICT operations and such operations can be conducted from any point on Earth, technological capabilities are unevenly distributed. This creates security risks. Consequently, the 2010 GGE report recommended (identification) of measures to support capacity-building in less developed countries.[240] These 11 terse words have since expanded into one of the main points of UN discussions.

---

[239] Section E, Recommendation 2, *First Annual Progress Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, UN document A/77/275, 8 August 2022. https://documents.un.org/doc/undoc/gen/n22/454/03/pdf/n2245403.pdf

[240] Paragraph 18 (iv), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/65/201, 30 July 2010. https://digitallibrary.un.org/record/3964709/files/DSS_33.pdf



At the heart of the debate is the extent to which countries with advanced ICT capacities are under an obligation to assist those with less developed capacities, i.e. to engage in technology transfer. This is rendered more complex by the fact that many of the capacities in question are privately owned. The IT industry is torn: on the one hand, it has an interest in a stable and secure ICT environment, which speaks in favour of ICT capacity building; on the other hand, it cannot agree to making

technologies developed at great cost available for free, which speaks against it. Governments' positions often mirror these competing concerns.

The role of the United Nations in all of this is hotly contested. Some envisage a UN ICT agency, possibly modelled on the International Atomic Energy Agency. Others hold that ICT capacity building should be done bilaterally or in public–private partnerships, and that institutions already exist to serve in a clearing-house and coordinating function (e.g. the Global Forum on Cyber Expertise). The UN Secretary-General has noted that *in reference to implementation of the normative framework, a number of States underscored that capacity-building, including financial and technical assistance, should be a fundamental component of the scope of the [proposed future] programme of action.*[241] He has, however, not endorsed a UN role in ICT capacity building.

In its 2024 report on a mapping exercise to survey the landscape of capacity-building programmes and initiatives,[242] the UN Secretariat argued that *'capacity-building should remain*

---

[241] Paragraph 10, *Report of the Secretary-General on a Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security*, UN document A/78/76, 18 April 2023. https://documents.un.org/doc/undoc/gen/n23/110/82/pdf/n2311082.pdf

[242] See mandate in paragraph 46 of the annex to the *Second Annual Progress Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021 – 2025*, UN document A/78/265, 1 August 2023. https://documents.un.org/doc/undoc/ltd/n23/227/59/pdf/n2322759.pdf

a fundamental and cross-cutting pillar of all related discussions by States at the United Nations on information and communications technologies security,[243] but was careful to recommend only that *'in the light of the universal nature of the open-ended working group on security of and in the use of information and communications technologies, States are encouraged to use the dedicated intergovernmental process to further unpack how to avoid duplication with a view to the best possible matching of needs with resources'*[244] (thus eschewing a position on a UN role). In the meantime, the discussion is moving towards establishing a dedicated Global ICT Security Cooperation and Capacity Building Portal and a United Nations voluntary fund—details to be elaborated.[245]

[243] Paragraph 85, *Mapping Exercise to Survey the Landscape of Capacity-building Programmes and Initiatives within and outside the United Nations and at the Global and Regional Levels*, Paper by the Secretariat, UN document A/AC.292/2024/2, 24 January 2024. https://digitallibrary.un.org/record/4038066/files/A_AC.292_2024_2-EN.pdf

[244] ibid.

[245] See the recommendations in paragraphs 52 and 54 of the *Third Annual Progress Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, UN document A/79/214, 22 July 2024. https://documents.un.org/doc/undoc/gen/n24/217/49/pdf/n2421749.pdf

The future: regular institutional dialogue

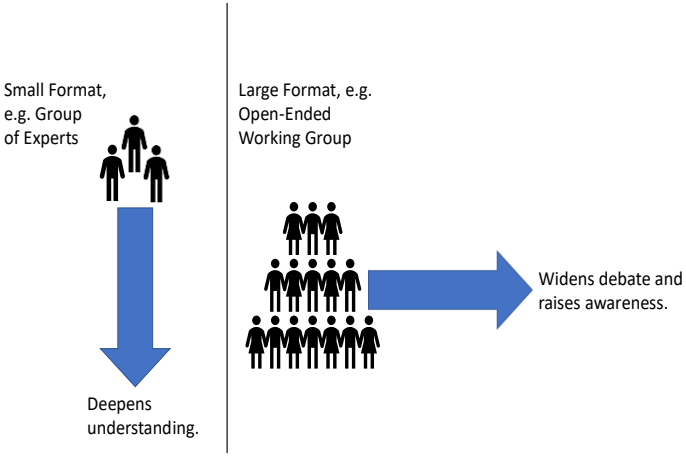
Various problems have beset the debate on ICT in the context of international peace and security. Some of the most prominent are:

- Lack of clarity what is being discussed: Is it the technical use of algorithms to manipulate, e.g. supervisory control and data acquisition systems of critical infrastructures? Or is it the content of electronic messages?
- Variation of focus: Digitally advanced actors have concerns that are very different from those of states with no or limited capabilities: The former want to agree the rules of state use of ICT, the latter focus on obtaining the capacities to recognise and fend off ICT attacks.
- Exclusion of key actors: Some non-state actors hold significant capabilities. However, in debates pertaining to international peace and security, they are sitting at the observers' desk—if they have a place at all.[246]
- De-facto veto for spoilers: From the outset, UN negotiations on ICT in the context of international security have been suffering from the United Nations' modus operandi: The GGEs were mandated to produce consensus reports. Lack of agreement was the reason, why in 2006 and

[246] The participation as observers of non-governmental organisations in OEWG meetings is a regular point of controversy at the UN. The IT industry, which shapes the ICT environment, holds some of the most advanced capabilities, but is not participating at all, or at best is participating indirectly, through industry associations.

2017, two such groups did not produce an outcome. This problem persists and is aggravating, as the discussion is moving into other forums with a wider membership.

There is an inherent tension between inclusivity and exclusivity. Following the failure of the 2016–2017 GGE to produce a consensus report, the UN General Assembly (UNGA) decided to migrate the discussion gradually from a small, exclusive format to an inclusive one. Between 2018 and 2021, a GGE and an OEWG, in which all UN members were invited to participate, were working in parallel. Since 2022, the OEWG on Security of and in the Use of Information and Communications Technologies has replaced the string of six GGEs. Its mandate runs until 2025.



	Open-Ended Working Group	Program of Action	Another GGE	Working Body under auspices of 1st Committee	Disarmament Commission	Conference on Disarmament	Conference of States outside UN
Format	Inclusive	Inclusive	Exclusive	Half-way between exclusive and inclusive	Inclusive	Partially inclusive	Flexible
Mandate	As before, unless changed by UNGA	To be determined by UNGA or conference of States	As before, unless changed by UNGA	Review and give guidance for implementation of GGE recommendations	To be determined by UNGA	To be determined by UNGA	Set by conference participants
Starting point	Open	Theoretically open, but very likely GGE and OEWG reports	Theoretically open, but in practice past GGE reports	GGE and OEWG reports	To be determined by UNGA	Theoretically open, but very likely GGE and OEWG reports	As defined by participating conference participants
Decision making	Voting	Consensus (possibly voting on procedural matters)	Consensus	Consensus	Consensus (tradition)	Consensus	Consensus of those who accept outcome
Typical Outcome	Reports	Action as determined in POA mandate	Report to the UN Secretary General, which is then endorsed by the General Assembly	Report to the 1st Committee that may inform UNG resolutions	Rare	Rare	As agreed by participant States

The 2018–2021 OEWG arrived at thin conclusions compared to the GGE meeting in parallel. In the same vein, discussions in the 2021–2025 OEWG are torpid. Irrespective of the chair's efforts to introduce more interactive formats, e.g. dialogues with stakeholders and informal inter-sessional meetings, the so-called debates consist largely of reading prepared statements. This is not to say that the OEWG serves no purpose: it increases awareness and draws attention to the issue.

Various options have, at one point or another, been considered for taking the discussion on ICT in the context of international peace and security forward.

Under the headline *Regular Institutional Dialogue*, two of these options have been developing momentum: 12 countries[247] have proposed to make the OEWG a permanent body. The core of its mandate should be developing legally binding rules, norms, and principles of responsible behaviour of states and the creation of effective mechanisms for their implementation, as elements of a future universal treaty. Such a permanent OEWG should take decisions by consensus and *exclusively by*

[247] Belarus, Burundi, Cuba, the Democratic People's Republic of Korea, Eritrea, Myanmar, Nicaragua, Russia, Syria, Sudan, Venezuela and Zimbabwe.

states.[248] A far larger group,[249] by contrast, put forward the idea of a Programme of Action to advance responsible State behaviour in the use of information and communications technologies in the context of international security ... as a permanent, inclusive, action-oriented mechanism to discuss existing and potential threats; to support States' capacities and efforts to implement and advance commitments to be guided by the framework for responsible State behaviour, which includes voluntary, non-binding norms for the application of international law to the use of information and communications technologies by States, confidence-building and capacity building measures.[250]

---

[248] *Concept Paper on a Permanent Decision-making Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies*, 15 December 2023. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_paper_on_a__Permanent_Decision-making_OEWG.pdf

[249] Albania, Argentina, Australia, Austria, Belgium, Bulgaria, Chile, Colombia, Croatia, Cyprus, Czechia, Denmark, Dominican Republic, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Monaco, Netherlands, Norway, Paraguay, Poland, Portugal, Republic of Korea, Republic of Moldova, Romania, Senegal, Slovakia, Slovenia, Spain, Sweden, Switzerland, Tunisia, Türkiye, Ukraine, United Kingdom of Great Britain and Northern Ireland, Tanzania and United States of America.

[250] Resolution adopted by the UN General Assembly, UN document A/RES/77/37, 12 December 2022. https://documents.un.org/doc/undoc/gen/n22/737/71/pdf/n2273771.pdf

Given divergent views among member states, the Secretary-General compiled these views into a single paper,[251] concluding that *consensus decision-making and inclusivity [are] critical elements of regular institutional dialogue in this area*.[252]

The OEWG's 2024 annual progress report, agreed in July 2024, suggested a *single-track, state-led, permanent mechanism under the auspices of the United Nations, reporting to the First Committee* of the UNGA (in charge of disarmament and international security).[253] Taking as the foundation of its work the GGE and OEWG reports, this mechanism should operate on the principle of consensus. Though this recommendation represents an important step forward, important points of contention remain, including the mechanism's mandate: several member states[254] have already emphasised that they *interpret the mandate as containing elaboration of legally*

---

[251] *Report of the Secretary-General on a Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security*, UN document A/78/76, 18 April 2023. https://documents.un.org/doc/undoc/gen/n23/110/82/pdf/n2311082.pdf

[252] ibid., paragraph 47.

[253] Annex C: Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the Context of International Security, *Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, UN document A/79/214, 22 July 2024. https://documents.un.org/doc/undoc/gen/n24/217/49/pdf/n2421749.pdf

[254] Belarus, Burundi, China, Cuba, Eritrea, Iran, Nicaragua, People's Republic of Korea, Russia, Syria, Venezuela and Zimbabwe

binding obligations in the field of international information security[255]—a position likely to be challenged. Other open issues are how to involve non-state stakeholders—the business community, academia and civil society—and how to integrate the work under the future mechanism with the envisaged Global ICT Security Cooperation and Capacity Building Portal, as well as a possible United Nations voluntary fund to support ICT capacity building.

Given the unresolved problems mentioned above—lack of clarity, variation of focus, exclusion of key actors and a de-facto veto for spoilers—it will take considerable diplomatic effort to build consensus on how to take forward the United Nations negotiations on ICT in the context of international security.

Karsten Geier

Senior Cyber Diplomacy Adviser to the Geneva-based Centre for Humanitarian Dialogue

Karsten Geier is Senior Cyber Diplomacy Adviser to the Geneva-based Centre for Humanitarian Dialogue. Between 2013 and 2018, he was responsible for cyber and international security in the German Federal Foreign Office. He was a member of the 2014/2015 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context

[255] Statements in explanation of position on the adoption of the progress report of the open-ended working group as contained in A/79/214, UN document A/AC.292/2024/INF/5, 3 September 2024. https://documents.un.org/doc/undoc/gen/n24/254/18/pdf/n2425418.pdf

of International Security (GGE) and chair of the 2016/2017 GGE. Karsten Geier has served at numerous bilateral and multilateral posts and participated in OSCE and NATO-led missions.

Thoughts and ideas presented in this paper are personal. They express neither a policy of the German Federal Government nor a position of the Centre for Humanitarian Dialogue.

Cyber Capacity Building: A Primer for Diplomats

Robert Collett

Introduction

In late 2023, INTERPOL coordinated the arrest of 975 people suspected of involvement in cybercrime across 34 countries. A highlight of the operation was the detention in the Philippines of a senior figure from an online-crime group that Korean police had been seeking for two years.[256] Another success of the operation was the information it revealed about how criminal gangs are using AI to commit fraud, with victims of voice-cloning scams identified by law enforcement in the UK and a warning notice issued by INTERPOL to all forces. This is the modern face of policing: transnational criminal operations countered by specialist officers and international cooperation. While media reporting focused on the arrests and $300m in seized assets, this chapter is concerned with what preceded the operation: over two decades of international cybersecurity and counter-cybercrime capacity building (CCB).

[256] INTERPOL. (2023, December 19). *USD 300 million seized and 3,500 suspects arrested in international financial crime operation*. https://www.interpol.int/en/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation

Since at least the mid-2000s, institutions and individual experts have shared knowledge and skills with their peers through CCB. Activities prior the 2023 operation illustrate how such cooperation can contribute to states being better prepared to protect themselves, their citizens and other countries.

- In 2014, the Philippines began a CCB partnership with the EU and INTERPOL under the Global Action on Cybercrime (GLACY) programme. Activities included training for judges and police, as well as advice on cybercrime legislation. In the second phase of the programme, the Philippines was chosen as the GLACY+ regional hub for cybercrime training.
- In 2015, INTERPOL set up the INTERPOL Global Complex for Innovation with a Cyber Fusion Centre, in Singapore, staffed initially by officers from 23 countries.
- In 2018, following support from the GLACY programme, the Philippines acceded to the Budapest Convention on Cybercrime, which enables closer operational cooperation through harmonised legislation and procedures. The following year the Philippines invited programme experts to provide advice as the country drafted its first National Cybercrime Strategy, which was completed in 2022.
- In 2020, INTERPOL commenced a multi-year series of operations, funded by Korea, against online fraud. In parallel, Korea gave INTERPOL €1.3 million to build the capacity of forces in ASEAN to combat cyber-enabled financial crime. This included training, advice and networking between forces.

- In 2023, Korea was formally invited to accede to the Budapest Convention, having met the requirements for harmonised legislation and after expressing interest in accession.

When Korean police asked Filipino counterparts to help arrest their target in 2023, the necessary capacity—legislation, policies, procedures, training and points of contact—was in place for a successful outcome. To understand what might have happened if these were not in place, we can contrast the operation with an incident two decades earlier. In May 2000, the Philippine police detained a student, Onel de Guzma, for creating a virus that caused an estimated $5–10 billion in worldwide losses. At the time, local laws did not cover this type of cybercrime and prosecutors were forced to release him. The Philippines' own efforts have ensured that it is now much better prepared to deal with such cybercrimes, but CCB has played a valuable supporting role.

What is CCB and why is it needed?

There is no universally agreed definition of CCB, but there is broad agreement on its core feature: voluntary international collaboration—typically involving the transfer of knowledge, skills or capabilities—with the objective of strengthening the capacities that mitigate risks to the safe, secure and open use

of the digital environment.[257] Nor has the field reached a consensus on whether 'cybersecurity capacity building' or 'cyber capacity building' is the better term for its activities, so this chapter uses the abbreviation CCB to cover both options.

CCB is necessary because no country or organisation can protect its safe, secure and open use of globally interconnected ICT systems on its own: a cybersecurity vulnerability, or safe haven for criminals, in one country creates a risk for all. Furthermore, there is a wide global disparity—a digital divide—in the level of resources and capabilities that countries have in order to respond to cybersecurity and cybercrime challenges. It is only by narrowing this digital divide, through a combination of domestic initiatives and international CCB collaboration, that we will reach an adequate level of global cybersecurity readiness.

The example this chapter opened with illustrates these dependencies within an interconnected system. Yet a third of countries still lack cybercrime legislation.[258] Similarly, a third of countries are without a national Cyber Security Incident Response Team (CSIRT), which is a basic requirement for domestic preparedness and international cooperation in the

[257] Collett, R. (2021). Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. *Journal of Cyber Policy*, *6*(3), 298-317.
[258] Cybercrime Programme Office of the Council of Europe (C-PROC). (2022). *The global state of cybercrime legislation 2013 – 2023: A cursory overview*. https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jan-2023-public-v1/1680a99137

face of serious cybersecurity incidents.[259] These are stark indicators of the digital divide.

There are significant consequences to not narrowing the digital divide and helping all countries reach a basic level of cybersecurity readiness. Currently, an estimated 6% to 8% of global GDP is lost to cybercrime and the harms caused by cybersecurity incidents.[260] Developing countries are particularly vulnerable, because most if not all of the Sustainable Development Goals are dependent on digital technology and the ability of governments and citizens to trust it.[261] This is especially true for developing countries seeking to leapfrog older technologies and benefit from being early adopters of

---

[259] International Telecommunication Union (ITU). (2024, September 10). *Countries strengthening cybersecurity efforts, but increased action still required*. ITU. https://www.itu.int/en/mediacentre/Pages/PR-2024-09-10-Global-Cybersecurity-Index.aspx.

[260] Baldini G., Barrero J., Coisel I., Draper G., Duch-Brown N., Eulaerts O., Geneiatakis D., Joanny G., Kerckhof S., Lewis A., Martin T., Nativi S., Neisse R., Papameletiou D., Ramos J., Reina V., Ruzzante G., Sportiello L., Steri G., & Tirendi S. (2020). CYBERSECURITY OUR DIGITAL ANCHOR a EUROPEAN PERSPECTIVE. In I. Nai Fovino, G. Barry, S. Chaudron, I. Coisel, M. Dewar, H. Junklewitz, G. Kambourakis, I. Kounelis, B. Mortara, J. p. Nordvik, & I. Sanchez (Eds.), *Publications Office of the European Union* (No. JRC121051). Publications Office of the European Union. https://doi.org/10.2760/352218 ; *Cybercrime to cost the world 8 trillion annually in 2023*. (2024, November 17). Cybersecurity Ventures. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[261] Oceania Cyber Security Centre. (2022). *CYBERSECURITY AND SUSTAINABLE DEVELOPMENT: An intersectional analysis* [Report]. https://ocsc.com.au/wp-content/uploads/2022/08/Cyber-Security-and-Sustainable-Development-2022.pdf

solutions such as e-government, digital ID and mobile money services. Failure to help these countries protect themselves not only puts their own development at risk, but also creates new training grounds and vulnerabilities that criminals and adversaries will exploit to target developed countries.[262]

Responding to the need for CCB, all members of the International Telecommunication Union (ITU) agreed in 2007 that it should be one of the five strategic pillars of a new Global Cybersecurity Agenda. More recently, this consensus support for CCB was reinforced by the 2021 final report of the UN Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security. The report finds that CCB 'helps to develop the skills, human resources, policies, and institutions that increase the resilience and security of States so they can fully enjoy the benefits of digital technologies' and recommends the promotion and resourcing of CCB efforts.[263]

---

[262] Schia, N. N., & Willers, J. O. (2021). Digital vulnerabilities and the sustainable development goals in developing countries. In *Encyclopedia of the UN sustainable development goals* (pp. 1–10). https://doi.org/10.1007/978-3-319-71059-4_115-2

[263] United Nations. (2021a). Final Substantive report. In *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

Why is CCB an issue for diplomats?

Engaging with CCB has been both a necessity and an opportunity for ministries of foreign affairs (MFAs). As the stewards of international relationships, MFAs were often expected to approve new training or exercising activity between their own government's officials and those of partner countries. Furthermore, when governments chose to launch their own CCB programmes they frequently turned to their MFA to administer it or lead an inter-agency coordination process for it. In addition to internal drivers, MFAs have needed to respond to external requests from partner countries and international organisations to include cybersecurity in dialogues and provide practical assistance through CCB.

Internal and external drivers made engaging with CCB a necessity for MFAs but, far from being passive in this process, they have actively seized the opportunity to use CCB and influence its development. One of the responsibilities of diplomats is to scan the horizon for international risks and potential solutions. By 2010, it was clear to several MFAs that the cybersecurity threats all countries faced were growing faster than the global response. There was no large-scale platform for the international community to discuss responsible state behaviour in cyberspace and CCB investment had increased little since the Global Cybersecurity Agenda had agreed the need for it in 2007.[264] In response, the UK held the

[264] Although a small group of national experts had been meeting through the UN Group of Government Experts since 2004 and the

first meeting of what would become the biennial Global Conference on Cyberspace (GCCS). At this inaugural event in 2011 the participating countries and stakeholders reaffirmed their commitment to capacity building, and several MFAs launched new CCB programmes soon afterwards.[265]

As investment in CCB increased after 2011, so did the need for coordination and sharing knowledge about best practices, and again MFAs played a pivotal role in advancing solutions. When the Dutch MFA hosted the GCCS in 2015 it used the event as a springboard to launch the Global Forum on Cyber Expertise (GFCE) as a multistakeholder community for CCB. The Dutch MFA has provided most of the GFCE secretariat's funding since, although the organisation now has independent charitable status and is diversifying its funding sources.

The influence of diplomats on CCB entered a new phase in 2019 with the launch of the UN OEWG. As mentioned, the final report of the first round of OEWG meetings in 2021 gave strong endorsement to capacity building. The report also contained 10 principles that states agreed to follow when engaging in CCB. As the second round of OEWG meetings nears its end in 2025, diplomats are now negotiating potential new mechanisms for advancing CCB within the orbit of the UN. In these negotiations

---

annual Internet Governance Forum was a convening space for civil society and government officials concerned with the governance of cyberspace.

[265] In 2012, the UK launched its first CCB activity under the National Cyber Security Programme, and the EU made its first use of the Instrument for Stability (later renamed the Instrument Contributing to Stability and Peace) for CCB. Canada followed in 2014 and Australia in 2016.

momentum is building for a UN Programme of Action to identify needs, mobilise resources and coordinate activity for CCB. To what extent this might be a multistakeholder mechanism and how it would fit with existing processes and organisations, such as the GFCE and ITU, is not yet clear.

Diplomats bring valuable skills, networks and resources to CCB, but they are only one of several policy and technical communities actively engaged in the field. Members of the justice sector, incident response and military communities were providing training for their colleagues in other countries years before MFAs began contributing to CCB. They work closely with the private sector companies responsible for most ICT infrastructure and the cybersecurity services that prevent incidents and handle them. These companies also volunteer for and fund CCB. In addition, there are active development banks, international organisations, regional economic communities, philanthropic foundations, universities, think tanks and many civil society organisations. Whereas the largest MFA CCB budgets are measured in tens of millions, the Inter-Americas Development Bank has a cybersecurity lending portfolio of $165m.

Diplomats are likely to continue to have a central role in the development of CCB but, as discussed further in the next section, a multistakeholder and multidisciplinary approach will be necessary to work with the other communities that are essential to the field.

Lessons from MFAs working on CCB

MFAs can have a wide range of responsibilities in relation to CCB, including administering capacity building programmes, finding or vetting new international partners, using CCB to support national policy objectives, incorporating CCB into bilateral relationships, coordinating CCB activity across their own government and with external actors, and contributing to the future development of the field. The following are lessons specific to MFAs that they have shared from this experience.

Coordinate a cross-government approach through committees, plans, programmes and embassies

Capacity building delivers the best outcomes when there is a nationally coordinated approach. This applies to countries that fund CCB programmes, those that request CCB support and those that do both. The responsibility for coordinating the offers or requests for CCB will often fall to an MFA.

An early step in coordination can be establishing an inter-agency committee for CCB, either as a stand-alone endeavour or as a subcommittee of an existing process. Giving the central government office and the lead technical agency (e.g. the National Cyber Security Centre) a prominent role on the committee alongside the MFA can help secure buy-in and expertise.

A cross-government CCB committee can be tasked with preparing a national CCB plan. This can guide the priorities and objectives of future programmes the country funds and/or prioritise the country's requests for CCB. Outputs from the planning process can include sections on CCB within national strategies and international cybersecurity policies or letters to potential partners and coordinating platforms, like the GFCE, setting out a country's requirements.

For countries that fund or deliver CCB, bringing activities together under a single programme can be an effective way to improve coordination. It standardises CCB processes across government and makes it easier to spot where there are connections to be made between different activities in the same country or thematic area. Donor countries have also made use of their embassies as platforms to coordinate inter-agency CCB activity and develop local CCB plans and proposals. Several US Embassies have gone a step further by inviting representatives of the host government and partner countries to join their inter-agency CCB coordination meetings. This contributes to both transparency and better donor coordination. MFAs in countries seeking CCB could similarly convene their own meetings of CCB donors and implementers to improve coordination, monitor progress and discuss future priorities.

Build partnerships with experts outside government

Much of the technical expertise for designing, delivering and de-risking CCB resides in organisations outside of government, so external partnerships are essential for MFAs to work effectively on CCB. Typically, these partnerships will look different with non-profit entities and commercial ones. Using grants, MFAs can form long-running partnerships with universities, think tanks, international organisations and civil society organisations. To build close partnerships with commercial companies, MFAs can invite them to co-sponsor programmes, run regular workshops open to all implementers or create supplier frameworks that make it easier to work with pre-validated firms.

Some examples of long-running MFA partnerships are the abovementioned EU collaboration with the Council of Europe and INTERPOL through GLACY, the UK Foreign Office's partnership with Oxford University's Global Cyber Security Capacity Centre on a national capacity maturity model, and the US State Department's partnerships with two federally funded research and development centres, MITRE and SEI.

In the UK, regularising annual 'implementer days' improved networking between UK-based companies involved in capacity building, who are now meeting independently and collaborating on non-papers to inform British capacity building. The EU is similarly supporting networking between its capacity

builders and strengthening its own CCB ecosystem through the CyberNet programme.

Professionalisation through training, processes and toolkits

As the CCB budgets of MFAs have grown, their staff have had to apply increasingly sophisticated programme management approaches, skills and lessons. Writing in 2021, this author and Nayia Barmpaliou described this process as being part of the professionalisation of CCB.[266]We saw a shift away from short, top-down, fly-in fly-out projects to larger, longer, demand-driven programmes, using local experts in the design and delivery. MFAs were also adopting well-established methods in international development, such as results-based management, end-to-end human rights risks management and sensitivity to gender and inclusion.

The professionalisation of CCB within MFAs continues and is driven by deliberate efforts such as trainings, updating processes and producing new toolkits to encourage lessons learning and the uptake of good practices. The EU is one of the best examples of this, having commissioned a handbook for its cyber capacity-building programme managers as early as 2018 and now investing in CCB training for its country office staff

[266] Collett, R., & Barmpaliou, N. (2021). INTERNATIONAL CYBER CAPACITY BUILDING: GLOBAL TRENDS AND SCENARIOS [Print]. In *European Union Institute for Security Studies*. European Commission. https://doi.org/10.2815/06590

through an ongoing series of regional trainings that began in 2022.[267]

Part of the early professionalisation trend within CCB was a move away from capacity substitution towards capacity building. Broadly that trend continues, but the conflict in Ukraine has elevated the question of how countries can respond when there is a short-term and urgent need for assistance from a partner. In such a scenario, substituting or augmenting domestic cybersecurity capacity with international resources may be required. The need for rapid emergency assistance also arises at other times of crisis, such as following a natural disaster. Whether such emergency support should be considered a form of CCB—and therefore subject to the same principles and addressed in the same forums as other CCB activities—is something the international community still has to determine.

Collaborate with other MFAs on CCB

MFAs have found several ways to collaborate on CCB. Arguably the most important have been the successful efforts to agree that CCB is a necessary global endeavour for strengthening global resilience and enabling the benefits of ICTs (cf. the Global Cybersecurity Agenda, Global Conference on Cyberspace and OEWG mentioned above). These agreements

[267] European Commission. (2018). International Cooperation and Development Operational Guidance for the EU's international cooperation on cyber capacity building. In *European Commission*. https://doi.org/10.2815/38445

pave the way for MFAs to collaborate on CCB, starting with coordination.

MFAs coordinate their CCB activity with one another in many ways. They use bilateral dialogues, likeminded groups, regional economic communities and other regional platforms, the GFCE and its regional hubs, and more recently the UN OEWG. Importantly, these coordination mechanisms work best when they include all relevant actors, not just diplomats.

As there are several ways in which coordination can occur, it helps to have a single place where any organisation involved in CCB can post information about its activities. The Cybil Portal was launched for this purpose in 2017.[268] It now holds information on nearly 1000 projects, plus 500 tools or knowledge products.

For some MFAs, the next stage in collaboration has been to jointly support specific CCB programmes or activities. This can be through co-funding or co-designing a project, contributing to a multi-donor trust fund or providing in-kind assistance such as speakers for a training event.

The latest evolution in MFAs collaborating on specific projects has been to use capacity building to help fellow diplomats engage in cyber diplomacy, especially where they are from under-represented groups. The Women in International Security and Cyberspace Fellowship is co-funded by six MFAs to help female diplomats attend and participate in UN OEWG

[268] *The Knowledge Portal for Cyber Capacity Building*. (n.d.). Cybil Portal. https://cybilportal.org/

meetings, through logistical support and training in negotiating skills and subject knowledge. This project has assisted diplomats from 42 countries and exemplifies the ethos of the earliest CCB projects: experts using their own experience and resources to support peers in other countries.

Looking ahead: issues for diplomats working on CCB

Doing more through the UN without duplication or excluding stakeholders

One of the consensus issues emerging from the UN OEWG is that there should be continued work on CCB within a follow-on UN process, whether that be in the form of a Programme of Action or something else. There are potential benefits to CCB from greater UN engagement, but there are also significant risks. Diplomats have a responsibility on behalf of all the communities involved in CCB to understand and address both.

The greatest benefits and lowest risks from a post-OEWG process for CCB would come from working with the UN's strengths: building high-level political support for an issue and maximising the use of UN agency capabilities. The UN can be a powerful tool for awareness raising, fundraising and agreeing global principles and priorities among states. Furthermore, the UN agencies themselves possess CCB experience, knowledge and resources that could be better coordinated and leveraged with the support of a post-OEWG UN process.

The greatest risks to CCB from a new UN process stem from proposals that it should take a more 'hands-on' role in directing, coordinating and keeping track of all CCB activity. CCB is an essentially multistakeholder field consisting of several different communities of practice. Many of these communities have already developed their own knowledge sharing and coordination mechanisms, while the GFCE and Cybil Portal are open, multistakeholder platforms for both intra- and inter-community coordination. There is a significant risk that any new UN 'hands-on' process would duplicate or cut across these existing efforts rather than empower them.

To avoid these risks, the post-OEWG UN process could focus on mobilising support for CCB, enhancing existing UN agency efforts and helping governments find and access the sources of support and information that already exist. However, if a post-OEWG process does choose to take a more 'hands-on' role, it will need to meaningfully engage with, and include, CCB's various communities and stakeholder groups to collect information and influence their activity. Such a multistakeholder approach would be in line with the Secretary-General's call for more inclusive and better networked multilateralism and follow the precedent of the sustainable development agenda in giving an enhanced role to Major Groups and other Stakeholders (MGoS).[269] it would likely face

[269] *Secretary-General's remarks at the Opening Segment of the Summit of the Future Plenary [bilingual as delivered, scroll down for all-English and all-French] | United Nations Secretary-General*. (2024, September 22).
https://www.un.org/sg/en/content/sg/statement/2024-09-

sustained challenge from states such as Russia and Iran that want to shift influence over CCB away from multistakeholder forums and regional economic communities to UN processes where they have more influence.

Mainstreaming CCB into development

The development community has embraced digital technologies and services as enablers of sustainable development, but paid relatively little attention to the corresponding cybersecurity risks or the ways in which CCB can mitigate those risks and contribute to SDGs.[270] This blind spot allows cybersecurity risk to accumulate in donor programmes and the infrastructure, services and processes they help develop. Inevitably some of these risks will materialise as incidents in which services are disrupted, personal data leaked or human rights violated.

Although awareness of cybersecurity concerns is generally low among the development community, some organisations with a higher level of risk exposure or ICT experience have identified the issue and begun mainstreaming CCB into their operations and programming. The World Bank, for example, has made

22/secretary-generals-remarks-the-opening-segment-of-the-summit-of-the-future-plenary-bilingual-delivered-scroll-down-for-all-english-and-all-french

[270] Hathaway, M., & Spidalieri, F. (2021, November 1). *Report: Integrating Cyber Capacity to the Digital Development Agenda - the GFCE*. The GFCE. https://thegfce.org/tools/report-integrating-cyber-capacity-to-the-digital-development-agenda/

cybersecurity risk assessments and mitigating measures a requirement in all its lending for digital initiatives. In addition, the Bank established cybersecurity expert advisor positions, prepared guidance documents for non-specialist staff, commissioned knowledge products that would allow for better risk assessments and created a multi-donor trust fund for CCB to pool resources.

Mainstreaming CCB into development is the responsibility of the development community but should be a priority concern for diplomats too. Mobilising Overseas Development Assistance and development expertise for CCB would accelerate progress towards the shared goal of an open, free, peaceful and secure cyberspace. Diplomats are also well placed to make the case for CCB to their development colleagues, especially within governments where diplomacy and development sit within the same ministry. For example, in 2016, diplomats in the UK's Cyber Policy Department reached out to their development colleagues with a proposal for a joint programme that addressed both barriers to internet access and cybersecurity risks. The result was a £59m (€69m) Digital Access Programme with activities such as partnering with Kenya to secure e-government services[271].

[271] Chatham House. (n.d.). *Digital Access: Trust and Resilience*. https://www.chathamhouse.org/about-us/our-departments/international-security-programme/digital-access-trust-and-resilience; *Digital Access Programme (DAP) | Social Development Direct*. (n.d.). https://www.sddirect.org.uk/project/digital-access-programme-dap

Much of the groundwork for mainstreaming cybersecurity and CCB into development has been laid. Researchers have explored the benefits mainstreaming would bring and the reasons it has been slow to occur,[272] while leading development organisations have published guidance for how it can implemented.[273] Building on this work, the 2023 Accra Call for Cyber Resilient Development provides a high-level roadmap that diplomats and development organisations can follow. Several cyber ambassadors were instrumental in supporting the conference at which this call was launched—the 2023 Global Conference on Cyber Capacity Building in Ghana—and continued support for the call from MFAs will be needed to raise awareness among development colleagues and make progress on the agreed actions.

[272] Pawlak, P. (2014) 'Developing capacities in cyberspace', in Pawlak, P. (ed.) Riding the digital wave: The impact of cyber capacity building on human development, ISSUE, report nr 21; Schia, N. N. (2016). The Cyber Frontier: Digitalization of the Global South. *European Cybersecurity Journal (2)*, 82-94; Morgus, R. (2018). *Securing Digital Dividends: Mainstreaming Cybersecurity in International Development*. New America; Unwin, T. (2021). 'Cybersecurity'and 'Development': Contested Futures.

[273] European Commission. (2018). International Cooperation and Development Operational Guidance for the EU's international cooperation on cyber capacity building. In *European Commission*. https://doi.org/10.2815/38445; USAID Technology Division. (2021). *A year in review*. https://www.usaid.gov/sites/default/files/2022-05/USAID_2021_Digital_Download.pdf

Applying a principles-based approach to CCB

Through the UN OEWG all countries have agreed to apply a set of shared principles in their CCB activities. Additionally, many countries have committed to applying principles in their CCB activity through other initiatives such the GFCE's Delhi Communiqué (2017), the Freedom Online Coalition's Donor Principles for Human Rights in the Digital Age (2023), the Digital Impact Alliance's Principles of Digital Development (2016) or the Busan principles of effective development cooperation covering any use of ODA funding for CCB (2011). Each of these initiatives is tailored to a specific context, but they have a common core: be demand driven; focus on achieving sustainable results; be transparent and accountable; be inclusive and respect human rights; work in partnerships; and protect users and their personal data.

The principles of CCB complement and support several related policies that are common or graining traction among MFAs. Most prominent among these is respect for human rights. The European Commission produced guidance on how CCB supports and applies its wider human rights policies as early as 2015. More recently, Canada and The Netherlands have adopted feminist foreign policies and commissioned projects

and research that will help apply the principle that CCB should be gender-sensitive and inclusive.[274]

The issue for diplomats working in the CCB field will be how they individually and collectively apply and promote the principles they have agreed in the OEWG and connected initiatives. The earliest calls for a principles-based approach in CCB stemmed from a critique that some MFA-led CCB interventions were more interested in achieving foreign policy influence than in meeting the needs of partner countries.[275] Now that all states have committed to a principles-based approach through the OEWG—including that CCB should be demand-driven, results-focused and politically neutral—the onus is on diplomats to help operationalise this agreement.

When deciding how best to apply and champion a principles-based approach to CCB, diplomats can learn from other principles-governed fields, especially international development. Where commitments to internationally agreed principles have been sustained, there has typically been a supporting environment including awareness-raising activities,

---

[274] Ministerie van Buitenlandse Zaken. (2022, December 7). *Feminist foreign policy explained*. News Item | Government.nl. https://www.government.nl/latest/news/2022/11/18/feminist-foreign-policy-netherlands; Government of Canada. (2017). *Canada's Feminist International Assistance Policy*. GAC. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/priorities-priorites/policy-politique.aspx?lang=eng

[275] Pawlak, P. (2016). Capacity building in cyberspace as an instrument of foreign policy. *Global Policy*, *7*(1), 83–92. https://doi.org/10.1111/1758-5899.12298

an expectation that organisations will demonstrate how they are embedding the principles in their policies, guidance and training for managers and practitioners, and a mechanism for reviewing progress and sharing lessons. A principles-based approach is also more likely to succeed if it has broad-based, multistakeholder support within the field. As the OEWG's principles were negotiated between states, albeit with some external consultations, any post-OEWG process for its principles will need to be more inclusive of other stakeholders to broaden support.

Robert Collett

Consultant & researcher for international cybersecurity capacity building

Robert Collett is an adviser, writer and speaker on international cyber security capacity-building. From 2019 to 2020, he was the UK's first seconded senior adviser to the Global Forum of Cyber Expertise (GFCE). Prior to this he ran, and grew threefold, the UK's international cyber security capacity building programmes. Robert has a 17-year track record leading programmes and policy initiatives as a UK diplomat, working at the intersection of foreign policy, security and development. During this period, he gave evidence to a Lords committee, led the strategic communications for NATO's Provincial Reconstruction Team in Helmand and managed a series of challenging projects from de-mining to countering violent extremism and cyber security.

Rules of the Road: International Law Guiding State Behaviour in Cyberspace

Joanna Kulesza

Role of international customary law and IHL in regulating state behaviour in cyberspace

The United Nations General Assembly, recognising the application of international law both online and offline, underscored the universality of legal norms across diverse domains.[276] Within this framework, Article 38 of the Statute of the International Court of Justice stands as an essential reference, acknowledged not only for its significance in

[276] General Assembly, UN (2019). UN Doc. Resolution adopted by the General Assembly on 22 December 2018 [on the report of the First Committee (A/73/505)] 73/266. Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/RES/73/266). https://documents.un.org/doc/undoc/gen/n18/465/01/pdf/n1846501.pdf

international adjudication but also as a universally recognised catalogue of sources of international law.[277]

It is in this context that public international law serves as the primary legal framework guiding the conduct of states online and offline, indicating their rights and obligations in the international arena. Enshrined in various conventions, treaties and customary practices, it provides the foundation for regulating state behaviour and resolving disputes. Sources such as the United Nations Charter, treaties, customary international law and general principles of law inform the application of international law to states. It is crucial to recognise that international law primarily governs states and their interactions, rather than those between individuals or companies.

This distinction underscores the sovereign nature of states and the unique legal landscape in which they operate. Private individuals and companies are not directly addressed by international law, short of certain human rights guarantees and other special regimes, but may be subject to it indirectly through domestic legislation or the application of international agreements. States are therefore obliged to ensure enforcement of their international law commitments, norms and regulations in domestic legislation and guiding the actions of private actors operating within their jurisdiction. Soft law mechanisms, such as those addressing business and human rights concerns or the concept of corporate social responsibility, provide additional guidance for states and non-state parties in fulfilling their international legal obligations and

[277] See Shaw, M. N. (2014). International Law. United Kingdom: Cambridge University Press.

promoting responsible state behaviour. In addition to upholding their commitments towards e.g. human rights and facilitating international trade, states are tasked with ensuring compliance with international humanitarian law, which governs the conduct of armed conflict and seeks to minimise the impact of warfare on civilians and other non-combatants. These commitments apply both online and offline, with states acting as domestic guarantors of relevant international norms being implemented. Through these measures, states play a pivotal role in translating international legal norms into tangible protections for individuals within their jurisdictions while fostering a harmonised legal environment conducive to economic development and adherence to global norms.

Customary international law (CIL), as enshrined in Article 38 of the Statute of the International Court of Justice, serves as a cornerstone of legal authority for the Court and the broader theory and practice of international law. It comprises two main elements: uniform state practice and *opinio juris*, reflecting both the consistent behaviour of states and their belief in the obligatory nature of such behaviour. Only states possess the authority to shape customary international law, as they determine and practice the norms that eventually solidify into customary law. Their actions and consistent behaviour in various spheres, including cyberspace, contribute significantly to the formation and evolution of these legal norms. Central to enforcement of international law is the understanding that sovereign states willingly adhere to their legal obligations on the international stage. However, it's important to note that the catalogue from Article 38 is non-exhaustive. Since its adoption, the catalogue of sources of international law has grown to

include, among others, acts of states and soft law in its unique capacity. These are very important for this chapter since state positions on the application of international law in cyberspace are acts of state and allow us to identify the *opinio juris* accompanying state practice.

Therefore, for a norm to attain the status of customary international law, it requires not only consistent adherence by a wide range of states but also an indication, whether explicit or implicit, of their consent to it.[278] The evolution of digital communications and the unique structure of cyberspace have prompted a re-examination of the traditional understanding of international law as the exclusive domain of states, raising questions about the role of non-state actors in shaping global norms of responsible behaviour.[279]

Traditionally, consistency in state practice has been considered crucial as it demonstrates both a state's consent to be bound by the norm and its dissent when the norm is consistently objected to, possibly through an act of state such as a declaration. To circumvent the binding nature of a CIL rule, a state must persistently voice its objection. Any alteration to established CIL mandates a fresh state of practice, supported by evidence that *opinio juris* aligns with the new practice rather than the former one. Discussions on state practice cover thresholds for determining the necessary level of 'widespread'

[278] Barrett, K., 'Customary International Law', in *Oxford Research Encyclopedia of International Studies* (Oxford: OUP, 2020).
[279] Eggenschwiler, J., & Kulesza, J. (2020). Non-state actors as shapers of customary standards of responsible behavior in cyberspace. *Broeders D, van den Berg B, editor, Governing Cyberspace: Behavior, Power and Diplomacy*, 245-262.

action, the representativeness of participating states, and the duration of consistent practice required for CIL formation. *Opinio juris* remains subject to debate due to its inherent subjectivity, unless explicitly affirmed through official statements endorsing the legal necessity of the practice.[280]

While it is evident that international law applies in cyberspace, as the UN consensus reports have affirmed, the customary law below the threshold of armed conflicts is still being shaped by state practice. Given this current landscape, it becomes imperative to shift focus towards the development of international customary norms and the subsequent application of existing legal frameworks.

The application of international humanitarian law (IHL) in the context of cyberspace remains a cornerstone of international legal norms, particularly for actions that surpass a specific threshold of conflict. As affirmed by the United Nations Group of Governmental Experts (UNGGE) and subsequently endorsed by the United Nations General Assembly (UNGA) in 2015 and 2021, IHL is unequivocally applicable to cyberspace operations that qualify as armed conflicts. This affirmation underscores the binding nature of IHL on all states, ensuring that even in the digital realm, the established principles of humanity, necessity, proportionality and distinction are upheld. These principles serve to protect non-combatants and to regulate the means and methods of warfare, thereby mitigating the humanitarian impact of cyber operations during conflicts.

---

[280] Barrett, K., 'Customary International Law', in *Oxford Research Encyclopedia of International Studies* (Oxford: OUP, 2020).

Despite the robust framework provided by IHL for situations above the threshold of armed conflict, the complexities of cyberspace pose significant challenges to implementing legal norms in the context of cyberspace. The dynamic and rapidly evolving nature of cyber threats, coupled with the anonymity and transnational characteristics of cyber operations, complicates the attribution of actions and enforcement of law. Consequently, the reliance on pre-existing IHL provides a more immediate and universally accepted set of guidelines that can be adapted to the nuances of cyber conflict. This renders the treaty-based approach less effective in addressing the unique aspects of cyber operations, necessitating a reliance on the flexible and established norms of IHL to maintain international peace and security in the digital age. In light of these observations, creating any kind of a 'cyber warfare treaty' would face significant challenges. Verification of compliance is nearly impossible due to the anonymity and complexity of cyber operations. Cyber tools that are created for offensive purposes using the dual-use ICT technology, cannot be verified by any arms control regime.

Moreover, a cyber warfare treaty could inadvertently infringe on human rights, such as privacy and freedom of expression, by justifying extensive surveillance and control measures. The rapid evolution of technology further complicates the establishment of static legal frameworks. Hence, the dynamic and multifaceted nature of cyberspace renders a conventional treaty approach ineffective, necessitating reliance on existing frameworks like IHL, which provides adaptable and universally accepted principles for managing cyber conflicts.

In the context of contemporary international relations and cyberspace, we will explore the complexities of applying the customary international law paradigm. This discussion will encompass an examination of the unique challenges and opportunities presented by the digital domain.

Customary norms guiding state behaviour in cyberspace

In 2019 the UNGA approved Resolution 73/266, affirming the findings of the GGE as outlined in its 2013 and 2015 reports. Therein UN states emphasised that international law, particularly the United Nations Charter, plays a vital role in preserving peace and stability and fostering an open, secure and accessible ICT environment. The voluntary adoption of norms of responsible state behaviour can mitigate risks to international peace and security, with the potential for additional norms to emerge over time given the unique nature of ICT. Additionally, confidence-building measures can enhance trust among states, reducing the likelihood of conflict by enhancing predictability and reducing misperceptions. Furthermore, capacity-building assistance in ICT security was deemed essential for international security, empowering states for cooperative efforts and promoting peaceful uses of such technologies. These conclusions underscore the significance of international cooperation and collective action in ensuring a secure and peaceful digital landscape.

The framework of international law, as outlined in Article 38 of the Statute of the International Court of Justice (ICJ),

encompasses various norms and principles, including treaties, customary international law, general principles recognised by civilised nations, judicial decisions, and teachings of highly qualified publicists and eminent scholars.[281] Customary law, in particular, evolves from state practice supported by *opinio juris*, emphasising the critical role of both factors in shaping international legal norms and ensuring their recognition and enforcement globally.

Acts of state are well-established sources of international law, serving as evidence of customary state practice.[282] Fortunately, there is a growing number of state declarations regarding the application of international law to cyberspace. These declarations constitute legally binding acts of state, enabling us to ascertain the extent and comprehension of the principles of international law that are recognised as binding in cyberspace and how they should be applied.[283]

The number of states declaring their position on the applicability of international law to cyberspace has increased significantly in recent years. This trend reflects a growing awareness and recognition of the importance of legal norms in governing behaviour in the digital realm.

---

[281] UN, Statute of the International Court of Justice (UN Doc. A/RES/2/4, 1945).
[282] Degan, V. D. (2024). *Sources of international law* (Vol. 27). BRILL.
[283] For an updated repository of state positions see: https://cyberlaw.ccdcoe.org/wiki/Applicability_of_international_law. See also UNGA, *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information* (2021).

At the time of writing (2024) one international organisation, the African Union, and 28 states provided declarations on the applicability of international law to cyberspace, including 12 EU member states.[284] The topics addressed by the declarations include sovereignty; due diligence; non-intervention; prohibition on the use of force; state responsibility, also in other circumstances precluding wrongfulness; and the right to self-defence in cyberspace, containing references to countermeasures and necessity as well as retorsions. They also usually include refences to human rights and international humanitarian law as well the obligation to settle disputes peacefully.

Divergences between states are evident across domains and are carried over into the cyber context, particularly concerning issues such as self-defence versus non-state actors and self-defence into territory from which a third party is conducting armed attacks. Additionally, unique challenges emerge or are exacerbated in the cyber context, such as sovereignty concerns regarding interference with government functions and the threshold for use of force. Furthermore, issues such as due diligence as a preventive obligation and minimal damage as a sovereignty violation present unique considerations specific to cyberspace governance.[285]

---

[284] Idem.

[285] See Chatinakrob, T. (2024). Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty. *Chinese Journal of International Law*, *23*(1), 25-72. https://doi.org/10.1093/chinesejil/jmae005; and generally, Giovanna Adinolfi, Talita Dias, Duncan B. Hollis, Vera

The further development of underdeveloped or unsettled but presumably uncontroversial matters, such as inherently governmental functions, plea of necessity, and the scale and effects test for use of force, presents opportunities for consensus-building among stakeholders.[286] Additionally, the expanded and streamlined treatment of international law governing attribution is conducive to fostering agreement and clarity on attribution issues. However, significant expansion of the treatment of international human rights law, peaceful settlement of disputes, IHL and jurisdiction may require careful negotiation to reach consensus due to their complexity and potential implications. Furthermore, unaddressed topics such as international criminal law remain a challenge for consensus-building efforts and may require further discussion and deliberation among states.

These declarations represent a broad spectrum of perspectives and interpretations of international law, underscoring the complexity and diversity of approaches among states in the realm of cyberspace governance. Despite this diversity, they provide valuable insights for identifying specific principles and their application to cyberspace, facilitating a deeper understanding of the legal landscape in this domain.

Rusinova, & Barrie Sander. (2022). *INTERNATIONAL LAW AND CYBERSECURITY GOVERNANCE* (F. Delerue & A. Géry, Eds.). https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/fQBr45KY/international-law-and-cybersecurity-governance.pdf.

[286] See national positions from Finland (2020), Germany (2021) or Denmark (2023).

States breaching international law, whether customary or treaty-based, risk state responsibility as outlined in the International Law Commission's (ILC) draft report. This responsibility extends to actions violating established norms, encompassing both treaty-based and customary norms.

Sovereignty and state responsibility in cyberspace

In the complex landscape of cyberspace, the interplay between sovereignty and state responsibility is particularly significant for the application of international law. As nations grapple with the challenges posed by the digital age, the concepts of sovereignty, non-intervention and state responsibility present themselves as foundational principles guiding state conduct in cyberspace. This section offers a look into the dynamics between these principles, examining their implications for cyberspace and international relations.

Sovereignty, a fundamental principle of international law, traditionally results in a state's supreme authority over its territory and population.[287] In cyberspace, sovereignty extends beyond physical borders to encompass digital domains, encompassing control over internet activities and infrastructure within a state's jurisdiction. China exemplifies this approach,

[287] Schwarzenberger, G. (1955). The Fundamental Principles of International Law (Volume 87). In *The Hague Academy Collected Courses Online / Recueil des cours de l'Académie de La Haye en ligne*. Brill | Nijhoff. https://doi.org/10.1163/1875-8096_pplrdc_A9789028612426_03.

advocating for digital sovereignty as a means to safeguard national security and social stability.[288] Through strict and direct governance of all relevant internet resources, including infrastructure and protocols, China asserts state control over cyberspace, prioritising its sovereignty over individual freedoms.

In contrast, the European Union member states stress the need for keeping cyberspace open and free, and access to information and freedom of expression will be prioritised. However, the European countries support the application of existing international law and many EU members have issued their opinions on how the current international law applies in this new domain. Regarding other key players, Russia is advocating the development of a new legal instrument specifically addressing state cyber activities in the context of international security.

The United States fully endorses the application of existing international law, including IHL, to cyberspace. However, data protection, especially personal data, remains a significant challenge in the US when compared with applicable EU policies, most significantly the General Data Protection Regulation (GDPR). Furthermore, the US and Europe diverge in their approaches to active cyber defence. The US openly adopts an offensive 'defend forward' strategy, emphasising proactive measures to disrupt threats before they materialise. European Union member states, on the other hand, focus on enhancing

[288] Creemers, R. (2020). 'China's Conception of Cyber Sovereignty: Rhetoric and Realization', in D. Broeders and B. van den Berg (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy*,107–142.

resilience and defensive capabilities in order to protect their key national cyber assets. Several EU countries have declared the offensive cyber programmes, and have issued related military strategies and built cyber commands.

Yet despite these contrasts, violations of sovereignty, as stipulated in Article 2, Paragraph 4 of the UN Charter, can trigger state responsibility, underscoring the need for states to exercise caution and prudence in their actions. In cyberspace, where attribution of malicious activities can be challenging, the attribution of non-state actors' actions or omissions to defaulting states requires direct engagement with the technical and business community. This underscores the importance of international cooperation and information sharing in addressing cyber threats effectively.[289]

The interplay between sovereignty and state responsibility shapes the landscape of cyberspace governance, influencing state conduct and international relations. While sovereignty remains a cornerstone of international law, its application in cyberspace necessitates adaptation to the unique challenges posed by the digital age. Effective cyberspace governance requires a delicate balance between sovereignty, intervention and responsibility, guided by principles of collaboration, transparency, and respect for fundamental rights. By navigating these complexities with prudence and foresight, nations can work towards a secure and inclusive cyberspace for all.

---

[289] See Hessbruegge, J. (2004, March 14). *The historical development of the doctrines of attribution and due diligence in international law*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2408953.

Dr. Joanna Kulesza

Assistant Professor at the Faculty of Law and Administration at the University of Lodz, Poland & CEO of the Lodz Cyber Hub Research Center

Dr. Joanna Kulesza is an Assistant Professor at the Faculty of Law and Administration at the University of Lodz, Poland, where she also directs the Lodz Cyber Hub Research Center. Her academic focus is on cybersecurity, international law, and the concept of responsible state behavior in cyberspace. Kulesza explores how states manage digital threats while adhering to international legal standards, focusing on the intersection of state sovereignty and global digital governance. Dr. Kulesza has contributed to significant academic discourse and policy developments related to cyberspace, collaborating with international bodies such as ICANN, GFCE, and the Internet Governance Forum. She has also participated in the European Union Agency for Fundamental Rights' Steering Committee, enriching her understanding of human rights in the digital context.

Opportunities and Challenges of Establishing Cyber Diplomacy as a Core National Security, Economic, Human Rights and Diplomatic Priority

Christopher M.E. Painter

The field of cyber diplomacy as a foreign policy priority is relatively young and still developing. In 2011—less than 15 years ago—when I was appointed the first high-level diplomat dedicated to cyber issues and established the Office of the Coordinator for Cyber Issues in the Secretary's Office of the U.S. State Department (S/CCI), it was the first such office of a foreign ministry in the world. Shortly thereafter, President Obama released the International Strategy for Cyberspace, a cross-cutting whole-of-government strategy that melded substantive areas including cybersecurity, military, economic and human rights dimensions in cyberspace. Though several countries had previously released national strategies for cybersecurity or digital development, this again was the first national strategy focused on international policy issues and goals. At its launch, then Secretary Clinton said the range of cyber issues 'comprise a new foreign policy imperative for which the State Department

has been exercising and will continue to have a leading role' and that this effort would require 'patient, persistent and creative diplomacy'.[290] To be sure, there were many diplomatic efforts related to cyber and digital efforts before this time, including significant work in the United Nations, but this was first time the issue was given dedicated high-level attention and signalled that the range of cyber and digital issues had come of age.

Indeed, for many years, and even now to some extent, many senior policymakers in the US and in other countries viewed cyber issues as purely technical, law enforcement or perhaps military issues and not as core national security, policy or ultimately diplomatic ones. This has been exacerbated by many policymakers exhibiting discomfort or even fear of what they viewed as a complex technical issue. However, though some understanding of the technical 'trade space' is important, a policymaker does not need to be a 'coder' to understand the geopolitical implications and challenges of cyber threats and digital opportunities—just like senior policymakers need not be nuclear engineers to understand the geopolitical nature of nuclear policy.

Over the past decade or so this perception has changed significantly, though many challenges remain to mainstreaming cyber policy as a core diplomatic issue around the world. For

[290] Cybersecurity, including working with other countries, was also noted in Obama's 2015 National Security Strategy:https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf, pp. 12–13.

example, when S/CCI was created and I would meet with foreign governments, there were no counterparts in foreign ministries to meet with. Instead, I would often meet with senior officials in the president or prime minister's office, the ministries of interior or defence, or the deputy minister of foreign affairs (who would frequently enquire as to why the US created such a structure and how they might do it as well). Now, over 50 countries have created structures in their foreign ministries to deal with cyber and digital issues with varying mandates and structural placement. These structures have continued to evolve. For example, though S/CCI was de-prioritised during the Trump presidency, it was re-elevated and strengthened during the Biden presidency with the launch of the cross-cutting Bureau of Cyber and Digital Policy. The US held its first diplomatic 'whole-of government' dialogue in 2011 (with Japan); there is now a complex web of cyber dialogues between and among countries around the world.

Of course, this increasing recognition of cyber and digital issues as a foreign policy priority has been driven, in part, by our increasing reliance on cyber and digital technologies and the increasing recognition that cyber-attacks and intrusions, whether perpetrated by nation states or criminals, constitute a real threat to economic development, national security and human rights.

It has also been driven by increased leader-level attention to cyber issues and a myriad of debates on these issues in virtually every multilateral and regional policy forum. Still, while progress has been made, there is a long way to go before cyber issues are truly embedded as a sustainable foreign policy

imperative around the globe. Too often, even now, attention on these issues is episodic—driven by specific egregious malicious incidents—and subject to being subverted to the next bright shiny policy or even technical development (as important as it is, the often nebulous invocation of 'AI' and the shift of attention and resources to that topic is an example). Accordingly, both for those who have existing diplomatic cyber structures in their foreign ministries and for those who are labouring to create or strengthen them, I offer a few practical suggestions for elevating and mainstreaming these evolving issues.

Scope and placement

As noted, the existing cyber and related offices that have been established in foreign ministries around the world vary widely in their substantive mandate and placement within the foreign ministry hierarchy—many reside in the arms control and security departments, some in technical chains, and others are placed at a higher, cross-cutting perch. Though there is no silver bullet, and every country needs to accommodate its own bureaucratic structure, both an expanded cross-cutting mandate and high-level placement significantly advance prioritising and mainstreaming cyber-related issues.

Cyber and digital issues are cross-cutting and interdependent—comprising and impacting security, economic and human rights considerations. For example, some states use the guise of cybersecurity to suppress the expression and protected activities of their populace, and some advocate for

greater state control of internet governance to again aid more repressive practices. State-based cyber intrusions have security, economic and human rights impacts and detailing the rules of the road, or norms, to prevent them and taking collective responsive actions involves both security and other considerations. Debates in what appear to be purely security or economic forums often have wider implications, and stove-piped policymaking could lead to conflicting policies with unintended results. Accordingly, it is best not to treat these issues in 'silos of excellence' but to, to the extent possible, put them together.

When S/CCI was created its coordination responsibilities spanned the full spectrum of cyber-related issues to include security, economic issues, freedom of expression, and free flow of information and it worked with functional and regional bureaus across the State Department on these issues. Importantly, the new office was expressly not limited to 'cybersecurity' but recognised that cyber issues were cross-cutting and interdependent—with security, economic and human rights considerations. The relatively new Bureau of Cyber and Digital Policy (CDP) at State expressly builds on and expands that approach—coalescing parts of State devoted to cybersecurity and cyber stability, digital policy, human rights online and emerging technologies. Australia's cyber office in its foreign ministry has expanded over the years to cover digital and emerging technology issues. The French cyber and digital ambassador similarly has an expansive mandate comprising security, digital issues and countering terrorist use of the internet. Although more narrow mandates may be required in some countries, close coordination between the entities that

handle these related issues is indispensable both for effective policymaking and to ensure that the issues receive appropriate attention and profile.

Organisational hierarchy always aids in both prioritising an issue and signalling its priority to other agencies and the outside world. In addition, given that foreign ministries are highly diversified and organised on both regional and functional lines, and given that cyber issues are substantively cross-cutting and transcend regional boundaries, a cross-cutting and global placement of this function is important. S/CCI was placed in the Office of the Secretary for this reason and the new CDP Bureau is placed in the deputy secretary's office both to enhance its authority and not to pigeonhole it in one of the functional under-secretary chains of command.

At a minimum, again, coordination between sometimes disparate regional and substantive parts of a foreign ministry is important. For S/CCI, the deputy secretary mandated that each regional and functional bureau dedicate a resource to work with the office and be part of a department-wide coordination group that I chaired on a monthly basis. This significantly increased coordination and communication. As an aside, the title of the office or structure is also important. When S/CCI was being established I resisted any attempt to call it the Coordinator for Cybersecurity vice Cyber Issues—precisely because its mandate was much broader, as noted above. I also wanted to avoid people thinking we would fix their computers—some still did, but we couldn't.

Mainstreaming cyber issues in the bureaucracy

One of the most difficult things about establishing a new area of diplomatic focus is contending with the often entrenched existing bureaucratic structure, and attitudes that are geared towards and comfortable with traditional diplomatic issues and view newcomers as either a passing fad or a threat to their mandates or resources. Many foreign ministries are structured to deal with geopolitical issues that countries have encountered in the past; they are seldom equipped to embrace emerging issues, particularly if those issues are cross-cutting and don't fit neatly in the existing organisational buckets. While Michele Markoff, my former deputy and an accomplished cyber diplomat for many years before the office was established, liked to say that 'if you're not taking turf [in the bureaucracy] you're losing it' and one of the initial detailees in my office (a human rights specialist, no less) used to post quotes from *The Art of War* on the office whiteboard, you can often, as the saying goes, catch more flies with honey: at least honey and high-level buy-in. Again, coordination and a collaborative approach with existing players are essential. In addition to the coordination committee of all the department components described above there was a steering group composed of all the under secretaries and chaired by the deputy secretary in order to get department-wide buy-in on input into these, at that time, novel and new diplomatic issues.

Having a presidentially mandated International Strategy was also an important leverage point for establishing a new diplomatic priority. In addition, Wendy Sherman, the then

under secretary for political affairs who had jurisdiction over all the powerful regional bureaus, mandated that each of the regional bureaus create a regional cyber strategy for cyber issues, based on the International Strategy and working with my office. These regional strategies not only created ownership at the regional assistant secretary level but helped mainstream the issue in the department as a whole and aided us getting these issues as part of the agenda of high-level bilateral dialogues that previously did not touch on cyber or digital issues. Moreover, we put the authors of these regional strategies from the various regional bureaus in for awards, to both recognise their contributions and garner collaborative goodwill in the future. We also used the regional strategies to train officers at our embassies around the world on cyber issues.

Again, high-level support helped as the deputy secretary, then Jim Steinberg, directed each US post to designate someone to follow these issues. The trainings were first done regionally and then, for several years, were held with all the regions in DC covering a range of substantive topics. Though the US Foreign Service Institute (FSI) first declined to offer a course on cyber diplomacy—telling me it could just be a passing fad—happily FSI has now instituted a comprehensive course in concert with the CDP Bureau. We also had success presenting these issues at the annual chiefs of mission conference and other senior leadership trainings—again seeking to embed them as a mainstream foreign policy issue instead of a curious and possibly short-lived boutique pursuit. Of course, each ministry will have its own structure and programmes, but the larger point is that it is important to demystify these issues, make

them understandable to a traditional diplomatic audience, and work in collaboration vice competition with them to embed cyber and digital issues in their core programmes—particularly on a regional level. Much success can be attained if the existing structure views you as partners and not competitors. Of course, having a high-level champion (like the minister, deputy minister or secretary general) is very helpful as well—but given the current profile of cyber and digital issues a strong case can be made that this will aid in their success as well. And, if possible, advocating for high-level international strategy for your country that gives diplomatic efforts profile or, at least, a robust international section in a broader national cyber or digital strategy will also pay long-term dividends.

Inserting the foreign policy issues related to cyber and digital issues into the larger inter-agency governance structure is also vital. While ministries of interior, justice, defence and commerce, the intelligence community and others may have had a leading role in cyber policy for many years, diplomacy brings both a new perspective and new tools to the table. In the US, the International Strategy, a multi-agency effort, and White House coordination ensured that a new cyber-diplomacy office was fully integrated into US government decision-making. Also, the intra-State coordination group discussed above was expanded to include representatives from each of the relevant agencies and the whole-of-government dialogues with other countries, though led by State, included senior representatives of each of the key US agencies. The tools of diplomacy, including negotiation, building alliances against shared threats, capacity building and exerting diplomatic pressure are helpful to all the goals a nation is trying to achieve

in cyberspace and, again, complement the functions and mandates of other agencies. For example, when US financial institutions were being subjected to long term cyberattacks from Iran utilising essentially armies of compromised computers in other countries, one of the most effective tools to combat and mitigate the threat was diplomatic demarches to ask other countries who were unwitting hosts of these compromised computers to help us. And, as the EU 'diplomatic toolbox' illustrates, diplomatic actions and frameworks are important in responding to states who transgress appropriate state behaviour in cyberspace. Where coordinating structures already exist in other countries, it is vital that the foreign ministry be a player.

Leverage current events and embrace change

There is an old adage that you should never let a good crisis go to waste. Though maybe that is a bit crass, one of the recurring problems that I have bemoaned over the years is that cyber issues would get high-level policy attention whenever there was a major incident, but attention would quickly wane soon after it left the headlines. That has seemingly changed in the last few years, when cyber-based election interference, a host of nation-state-launched destructive malicious computer worms, cyber use in Russia's invasion of Ukraine and the virtual pandemic of ransomware has compelled senior policymakers, including foreign ministries, to pay attention in a sustained manner.

States are increasingly concerned about cyber tools in warfare or as a prelude to war and are aware of digital vulnerabilities. Disruptive acts such as ransomware have made cyber threats a more frontline political priority as everyday people are victims. On the other side of the coin, digital technologies are transforming the world and almost every country, including developing countries, which are betting their economic futures on digital transformation. Both the threats in cyberspace and the opportunities are the business case for why cyber and digital diplomacy is an essential part of every country's policy portfolio and an essential pursuit of a foreign ministry.

Negotiations on these topics are taking place in every diplomatic forum and the decisions being made will dictate both the response to threats and appropriate state behaviour and how to leverage emerging technology. Without a strong diplomatic presence, a country cannot adequately participate in these debates, shape the environment, thwart rising cyber threats or take full advantage of technological advancement. If this is not enough to bolster cyber and digital issues in your foreign ministry, you can turn to the increasing number of states that have embraced these issues as a foreign policy concern as an example.

Some concern has also been raised by existing cyber diplomats that new and emerging issues, such as Artificial Intelligence, will suck all the oxygen from senior policymakers to the detriment of their attention on budding and still vital cyber and digital issues. There is some truth to this, as AI poses many valid concerns while, at the same time, the term is used in such an amorphous way that it becomes all-consuming. Cyber and

digital diplomacy can and should accommodate and embrace this and other technological developments. Of course, AI will play a vital role in cyber defence and, sadly, cyberattacks, and diplomats with a background in cyber and digital issues are best equipped to deal with these issues. Again, these new threats and opportunities can serve as the basis for pouring more resources into cyber diplomacy if presented effectively.

Other suggestions

If you are building out a new cyber-diplomatic office or bolstering an existing one, a range of skills is necessary. Though you don't need to be a coder to engage in cyber diplomacy, it is good to have at least some part of the office that has technical expertise and can help evaluate the technical implications of proposed policies. For example, I had a senior technical advisor in my former office that was a former senior executive and helped invent the cell phone. (He, Len Hause, is still part of the CDP Bureau and is also an amazing harmonicist—though that is optional I suppose for the post.) In addition, it is good to have multistakeholder advisory bodies. Industry, civil society, academia and think tanks can provide invaluable perspectives, particularly in complex negotiations. Any cyber-diplomacy office requires a range of skills including negotiators, regional experts, subject matter experts—in short, traditional diplomatic skills are as important as substantive knowledge.

Take advantage of the growing network of cyber diplomats, including training opportunities like the Tallinn Cyber

Diplomacy Summer School. There are also international conferences devoted to cyber and digital issues, including geopolitical and diplomatic issues. Though there are seemingly so many cyber summits it's like the Cyber Alps, many of these meetings are helping shape current and future debates.

If you are appointed to be a cyber diplomat, engage and get involved at your earliest opportunity—don't be afraid of the issues. I recall one county's designated lead waiting six months before they felt comfortable engaging publicly—that is far too long given the huge amount of activity in this area. There are many existing resources to get up to speed. For example, one new cyber-diplomatic lead listened to several episodes of the *Inside Cyber Diplomacy* podcast and others simply talked to their counterparts. To me, one of the best examples was the Japanese cyber ambassadors who, though they changed frequently, always hit the ground running. I recall that at dinner following one of our US–Japan whole-of-government bilats I bemoaned to my then Japanese counterpart that they rotated to other posts in a short time. He laughed nervously and pulled me aside to say he was leaving the following week for a new post. But his replacement was every bit as accomplished and up to speed in a matter of a couple of weeks. That is the norm for diplomacy generally, and there is no reason it should be different for cyber diplomats.

Conclusion

Cyber and digital diplomacy is a young but quickly evolving and growing field. It is also filled with opportunities to shape the future and critical to international security, economic development and the protection of human rights. Unlike many established areas of diplomacy, even relatively junior officers can have a major impact in shaping policy because it is still evolving and not set in stone. The same is true for smaller countries, whose diplomatic voice can play a significant role in shaping cyber and digital policies around the world.

Perhaps, in 20 years, we will no longer be talking about cyber or digital diplomacy because it will be so mainstreamed into traditional security, economic and diplomatic policy that it is no longer considered distinct. That would be a welcome end-state but, until that time, there is much to do to prioritise these issues as a diplomatic issue in every country and create appropriate structures to take this work forward.

Christopher Painter

Former President of The Global Forum on Cyber Expertise Foundation and former US Cyber Diplomat

Christopher Painter is a globally recognized leader and expert on cyber policy and cyber diplomacy for over thirty years—first as a prosecutor of high-profile cybercrime cases, and then as a senior official at the Department of Justice, the FBI, the National Security Council and the State Department. During the Obama

presidency, as Senior Director for Cyber Policy in the NSC, he coordinated the first ever International Strategy for Cyberspace. Subsequently, he established and led the Office of the Coordinator for Cyber Issues at the State Department — the first high-level position and office in the world dedicated to advancing the diplomatic aspects of cyber issues including national security, incident response, public-private partnerships and human rights matters. Among other things, Mr. Painter served as the President of the Global Forum on Cyber Expertise Foundation, is a non-resident Senior Advisor at the Center for Strategic and International Studies, and an Associate Fellow at Chatham House.

The Future of Foreign Policy in the Age of Emerging and Disruptive Technologies

Raluca Csernatoni

Introduction

What are the foreign policy and national security implications of emerging and disruptive technologies (EDTs)? In January 2024, OpenAI quietly amended its usage policy, notably lifting explicit prohibitions on military applications such as 'weapons development' and 'military and warfare'. This is a significant move in the company's stance on military Artificial Intelligence (AI). The change has sparked ethical and responsible governance concerns about the potential ambiguity of this new policy regarding military uses of Generative AI (GenAI) applications. This alteration carries profound implications for geopolitical, national security and foreign policy dynamics, as it plays out against an escalating trend to integrate AI systems into military arsenals worldwide and deploy them on the battlefield.

The ongoing Russian war of aggression against Ukraine has been described as a 'super lab of invention' for new

technologies or an 'AI war lab'[291] that has allowed high-tech companies and entrepreneurs to test new tools directly on the battlefield. The conflict has revealed a major shift in how wars are fought, demonstrating that the boundaries between military and civil or commercial domains are becoming more porous and following non-traditional technological innovation routes. Israel's deployment of sophisticated AI systems[292] in its war on Hamas is another case in point, eliciting a plethora of international humanitarian law and ethical dilemmas while fundamentally reshaping the nexus between military human operators and machines.

The evolving geopolitical landscape underscores the imperative for diplomats and foreign policymakers to navigate the ethical and strategic dimensions of dual-use EDTs that can be harnessed for both civil and military purposes. As states, international organisations and corporate technological giants grapple with the twin imperatives of cutting-edge technological innovation and responsible governance, a deeper understanding is needed of the complex interplay between EDTs and global security paradigms. Although the impact of EDTs like AI on international affairs might seem to be the stuff of science fiction, of imagined futures either utopian or

[291] Bergengruen, V. (2024, February 8). How tech giants turned Ukraine into an AI war lab. *TIME*. https://time.com/6691662/ai-ukraine-war-palantir/

[292] Davies, H., & McKernan, B. (2024, April 3). 'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets. *The Guardian*. https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes

dystopian, the Fourth Industrial Revolution[293] triggered by the increasing fusion of new technologies is all too real.

Either to make sense of such sweeping changes or to raise the alarm, experts have been contending with how states increasingly 'weaponise interdependencies'[294] by leveraging global networks of informational and financial exchange for strategic advantage; how a global battle to innovate, but also to govern and regulate new technologies is being played out between 'digital empires' like the United States (US), China and the EU;[295] and how states are currently experiencing a 'technopolar moment'[296] as large technology companies rival them for geopolitical influence. Against this backdrop, the essay will examine the definitional nuances of EDTs and their transformative implications, highlight the role of corporate technological players in reshaping the global order, and, finally, explore the need to reimagine foreign policy in the twenty-first century.

---

[293] Schwab, K. (2016, January 14). *The Fourth Industrial Revolution: what it means and how to respond*. World Economic Forum. https://www.weforum.org/stories/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

[294] Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

[295] Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

[296] Bremmer, I. (2021, October 21). The Technopolar Moment: How digital powers will reshape the global order. *Foreign Affairs*. https://www.foreignaffairs.com/articles/world/ian-bremmer-big-tech-global-order

The impact of emerging and disruptive technologies

How are EDTs defined, and what is 'emerging' and what is 'disruptive' when it comes to new technologies? Disruptive technologies[297] redefine the status quo, fundamentally altering established processes. Coined in this sense by Joseph L. Bower and Clayton M. Christensen in their seminal 1995 Harvard Business Review article 'Disruptive Technologies: Catching the Wave',[298] the term 'disruptive' could encapsulate technological innovations like AI, quantum computing, autonomous robotics … and the list can continue.

A novel technology can assume one of two roles: sustaining or disruptive. Sustaining technology embodies incremental advancements on existing technological frameworks. In contrast, disruptive technology propels a paradigmatic revolution within its sphere of influence, promising both opportunities and risks corresponding with its transformative potential. According to the European Commission's 2021 'Action Plan on Synergies between Civil, Defence and Space Industries', the term 'disruptive technology' encapsulates 'a technology inducing a disruption or a paradigm shift, i.e. a

[297] Csernatoni, R., & Martins, B. O. (2023). Disruptive technologies for security and defence: temporality, performativity and imagination. *Geopolitics*, *29*(3), 849–872. https://doi.org/10.1080/14650045.2023.2224235

[298] Bower, J. L., & Christensen, C. M. (1996). Disruptive technologies: Catching the wave. *The Journal of Product Innovation Management*, *1*(13), 75-76. https://hbr.org/1995/01/disruptive-technologies-catching-the-wave

radical rather than an incremental change. Development of such a technology is "high risk, high potential impact", and the concept applies equally to the civil, defence and space sectors. Disruptive technologies for defence can be based on concepts or ideas originating from non-traditional defence actors and find their origins in spin-ins from the civil domain.'[299]

The North Atlantic Treaty Organisation (NATO) takes a slightly different approach, splitting the concept into 'emerging' versus 'disruptive' technologies, defining the former as reaching maturity during 2020–2040, and the latter as having a major, even revolutionary, impact on security and defence functions. It could be argued that emerging technologies represent innovative technologies that have been recently developed, are currently in progress, or are slated for development within the next few years.

In stark contrast, disruptive technologies herald seismic shifts, fundamentally redefining the operational paradigms of organisations and entire industries alike. Various lists highlight EDTs critical for national security and defence. For instance, NATO and its innovation activities at present focus on nine priority technology areas: artificial intelligence (AI); autonomy; quantum; biotechnologies and human enhancement; hypersonic systems; space; novel materials and manufacturing; energy and propulsion; and next-generation communications

[299] European Commission. (2021). *Action Plan on Synergies between Civil, Defence and Space Industries'*. https://commission.europa.eu/document/download/2353ded9-0e39-4d35-a46c-67c62779afe1_en?filename=action_plan_on_synergies_en.pdf

networks. The European Defence Agency (EDA) has identified six EDTs for their strategic implications: AI; big data analytics; robotics and autonomous systems; hypersonic weapon systems and space; new advanced materials; and quantum-based technologies. Invariably, AI systems are featured at the top of such lists.

For instance, established in 2018 by the US Department of Defense (DoD), the Joint Artificial Intelligence Center (JAIC)[300] aimed to harness AI's transformative potential for national security. Led by Lieutenant General John N.T. 'Jack' Shanahan, the JAIC ventured into uncharted territory, building on Shanahan's previous involvement in Project Maven, a controversial initiative exploring AI's role in military operations. Shanahan envisioned a collaborative approach, bridging military, academic and commercial sectors to pioneer AI solutions for modern warfare. Against the backdrop of US–China geopolitical tensions, the JAIC prioritised AI integration across defence operations, emphasising joint warfighting capabilities and civilian-sector AI advancements. The JAIC's evolution underscored broader shifts in DoD governance prompted by the disruptive effects of integrating AI systems and culminating in its merger with other digital-focused entities to form the Chief Digital and Artificial Intelligence Office (CDAO). The motto of the CDAO[301] is to 'accelerate DoD adoption of data, analytics, and artificial intelligence from the boardroom to the battlefield to enable decision advantage',

[300] Chief Digital and Artificial Intelligence Office (CDAO), (n.d.), Home. https://www.ai.mil/
[301] ibid.

underscoring the importance of the technology for the military field. This consolidation reflects the Pentagon's strategic pivot towards agile, cross-sectoral approaches to AI and data analytics. The CDAO's journey offers valuable insights into the complex interplay between military innovation, EDTs like AI, private sector collaboration and institutional adaptation, shaping US defence policy in an era of AI-driven warfare.

In the summer of 2023, the DoD announced[302] the establishment of a GenAI task force led by the CDAO and so-called 'Lima'. The task force was set to play a pivotal role in analysing and integrating GenAI tools across the organisation. When it comes to hybrid warfare, the recent proliferation and advancement of GenAI models can profoundly impact cybersecurity, but also reshape knowledge production and dissemination, offering both promise and peril. While GenAI algorithms can disrupt by generating copious amounts of content across various mediums, they also introduce significant risks, particularly concerning the spread of misinformation and disinformation. The ability to fabricate convincing fake news articles, manipulated images and deepfake videos challenges the veracity and credibility of information outlets. Especially in the context of elections, the dissemination of AI-generated misinformation poses a threat to democratic processes,

[302] US Department of Defense. (2023, August 10). *DOD Announces Establishment of Generative AI Task Force* [Press release]. https://www.defense.gov/News/Releases/Release/Article/3489803/dod-announces-establishment-of-generative-ai-task-force/

potentially influencing public opinion and eroding trust in political institutions.

Overall, war has historically always catalysed technological disruptions, as recently exemplified by the collaboration between foreign civilian high-tech companies and the Ukrainian armed forces. This is propelling novel and unprecedented experimentation with EDTs like military AI on the battlefield. While questions remain on whether these public–private dynamics are poised to accelerate a profound shift in the very nature of warfare, they certainly mark a milestone in corporate-led military innovation. The war in Ukraine underscores the blurred boundaries between military and civilian technological domains, with non-traditional innovation pathways gaining prominence. Zooming out from Ukraine's case, the absence of globally acknowledged governance frameworks for military AI poses a pressing diplomacy concern. Moving forward, diplomats will need to carefully navigate international fora while promoting inclusive collaboration among states, international organisations and various stakeholders to mitigate the complexities of military AI responsibly and ethically.

The role of Big Tech

Are corporate technological giants overtaking states' authority? As previously outlined, AI is widely recognised as the defining technology of the twenty-first century, crucial for geopolitical competition and the future of national security. For example, unlike earlier periods, the Pentagon is no longer at the forefront

of research, development, investment and innovation in EDTs such as AI. Instead, Big Tech companies, which generate most of their revenue from non-defence sources, now employ most AI talent, control vast amounts of computing power and data and invest the most capital in improving AI algorithms.[303] Consequently, the Pentagon has sought closer and more effective collaboration with Silicon Valley firms, prompting changes in institutional structures, organisational culture and the required skillsets and mindsets. These changes also reflect a change in the balance of power within an emerging military–commercial complex that is renegotiating power dynamics between governmental, military and commercial tech establishments. The shift of power from states to Big Tech in the realm of EDTs marks a significant reconfiguration of sovereignty. Traditionally, governments led the charge in technological advancements, but today, tech giants like Google, Apple, Amazon, Nvidia and Microsoft, to name a few, are at the vanguard. These companies, mostly situated in the US or China, command vast resources, attract top talent, and drive innovation at an unprecedented scale, leaving state-led initiatives trailing.

In terms of another example, the impact of quantum technologies on humanity, including in the areas of security and defence, is far-reaching. Important applications in all domains of warfighting include, but are not limited to,

[303] Voss, N., & Ryseff, J. (2022, June 9). *Comparing the organizational cultures of the Department of Defense and Silicon Valley*. RAND. https://www.rand.org/pubs/research_reports/RRA1498-2.html

computing, encryption, problem optimisation, positioning and timing, sensing, and communications. In the fields of security and defence, quantum technologies are disruptive for various reasons: quantum computing breaks many of the encryption algorithms that could compromise the security of sensitive information, data and communications; quantum systems provide new methods for securing communications; quantum sensors are capable of detecting very small changes in gravity, magnetic fields and other physical properties, thus making them extremely valuable for detecting stealth submarines and aircraft; quantum computers may solve certain optimisation problems much faster than classical computers, especially in areas like military strategy and logistics; and quantum technologies can provide more precise positioning and timing data than traditional Global Positioning System (GPS). All these factors have the potential to radically transform traditional (cyber)security and defence practices and entail new approaches to design and control.

Big Tech's dominance in AI and quantum computing means it increasingly sets the agenda in these critical areas. The race for quantum supremacy is still on between companies like IBM, Amazon, Google, Microsoft, Huawei and Baidu. All have recognised the potential of a new quantum-enabled technological revolution, and have committed substantial funds to the research, development and fielding of quantum technologies. A crucial dimension of a potentially quantum-disrupted future will be to assess global trends in the quantum ecosystems, and who will be profiting from the innovation and commercialisation of dual-use quantum technologies and for

what purposes, especially in a landscape surrounded by secrecy and dominated by a limited number of commercial giants.

Their financial clout and rapid innovation cycles outpace the slower, more bureaucratic processes of government research and development. This transition is not merely about economic power but extends to regulatory and policy influence on the global stage. Tech companies lobby extensively, shaping legislation and standards to their advantage, often leading to regulatory frameworks that align with their interests. For instance, tech giants have also put forward various AI principles, from Microsoft's Azure AI Principles, which offer a guide for the development and application of AI in the company, to Google's Ethical AI Principles, which serve as a framework for evaluating new AI products and features. Other examples include Amazon's commitment to the responsible use of AI technologies, OpenAI's approach to AI safety, and the World Economic Forum's Global AI Governance Alliance, an initiative that unites industry leaders, governments, academic institutions and civil society 'to champion responsible global design and release of transparent and inclusive AI systems'.[304]

To delineate the corporate ethical AI agenda, three broader regulatory strategies are possible: first, an absence of legal regulation, with ethical principles and responsible practices relegated to voluntary and non-binding commitments; second, a middle ground involving soft regulatory frameworks that do not substantially conflict with innovation and profitability; and

[304] World Economic Forum. (n.d.). *AI Governance Alliance*. https://initiatives.weforum.org/ai-governance-alliance/home

third, hard regulation that restricts or prohibits the deployment of the technology. Predictably, the tech sector leans towards the first two options and resists the third. This is further exemplified by the Tech Accord to Combat Deceptive Use of AI in 2024 Elections, signed by 20 companies, including Adobe, Amazon, Google, IBM, Meta, Microsoft, OpenAI, TikTok and X, and announced during the 2024 Munich Security Conference.[305] While it is promising to see that such companies acknowledge the wide-ranging harms posed by generative AI, the principles proposed under the accord are generic and reactive and do not proactively address the potential weaponisation of content that is deceptively fake or alters the appearance, voice or actions of key political figures during elections. The accord's commitments are declaratory and lack nuance in terms of defining harmful AI-generated content, disinformation and weaponisation.

As Big Tech takes the lead in these sectors, traditional notions of state sovereignty are challenged. Governments now find themselves in a reactive position, seeking partnerships with these corporate behemoths to maintain a semblance of influence. This shift underscores a new era where technological sovereignty[306] in EDTs is increasingly defined by corporate

[305] Munich Security Conference. (2024). *A Tech Accord to Combat Deceptive Use of AI in 2024 Elections*. https://securityconference.org/en/aielectionsaccord/

[306] Csernatoni, R. (2022). The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty. *European Security*, *31*(3), 395–414. https://doi.org/10.1080/09662839.2022.2103370

capabilities rather than state control, which profoundly shapes how states engage in international affairs.

Foreign policy reimagined?

While Big Tech companies increasingly shape global affairs, governments must rethink their foreign policy tools to counter this growing influence. There are several approaches that states can embrace to reaffirm their influence and ensure a balanced global power dynamic. Governments must enhance their regulatory frameworks to better anticipate and mitigate the activities of Big Tech companies and the negative disruptive effects of the EDTs researched, developed and deployed by such corporate players in both civil and military domains. This involves updating antitrust laws to address the unique challenges posed by digital monopolies. International cooperation is also crucial in countering the global influence of technological giants. States and international organisations like the EU should collaborate to create a harmonised regulatory approach that prevents tech companies from exploiting regulatory grey areas, where they take advantage of more lenient laws in certain jurisdictions. International organisations and forums like the Council of Europe, OECD, G7, G20 and the United Nations can be instrumental in nurturing such collaboration. A robust global technological governance framework could align regulations on data privacy, human rights protection, content moderation, knowledge production and circulation, trustworthy AI and dual-use technologies,

ensuring a level playing field and mitigating technological divides.

Technological or digital sovereignty involves reclaiming a modicum of control over national digital infrastructures, as well as navigating the innovation and governance of EDTs in new and agile ways.[307] Governments and institutions like the EU and NATO should boost tech industries to reduce reliance and critical dependencies on foreign tech giants, especially in key domains such as AI, quantum, semiconductors, autonomous robotics and biotechnologies. This can be achieved through public funding for research and development, public–private partnerships, fostering innovation hubs and supporting local startup communities. Moreover, developing national digital services and platforms can offer alternatives to services provided by Big Tech, thereby reducing its market dominance. Public procurement policies can be leveraged to promote competition and innovation. Strengthening cybersecurity is equally essential in protecting national interests. Governments should develop robust cybersecurity strategies to safeguard critical infrastructure and sensitive data from potential misuse or AI-driven and increasingly sophisticated cyberattacks. Collaboration with other nations on cybersecurity standards

[307] Csernatoni, R., & Avar, F. (2023, November 13). *Navigating the Future: The EU's blueprint for the innovation and governance of emerging and disruptive technologies*. EU Cyber Direct Digital Dialogue. https://eucyberdirect.eu/research/navigating-the-future-the-eu-s-blueprint-for-the-innovation-and-governance-of-emerging-and-disruptive-technologies

and practices can also help mitigate the risks posed by the concentration of digital power.

Importantly, governments should promote the development and use of technology that aligns with ethical standards and public interest. Establishing national and international ethical guidelines for AI and other emerging technologies can ensure that their deployment respects human rights and democratic values. By setting such standards, governments can influence global tech practices and mitigate the potential harms of unregulated, unethical and unsafe technological advancement. Overall, in an era defined by great power rivalry and tech competition between Big Tech giants, foreign policy and tech diplomacy must evolve into a more agile and multidimensional approach. Governments should establish a 'tech-savvy diplomacy corps' dedicated to navigating the complex intersections of technology and international relations. Also, by integrating technology into the core of foreign policy, states can navigate the complexities of the digital age, balancing innovation with security, and ensuring a competitive yet cooperative global tech ecosystem.

Conclusion

Technological corporate giants are reshaping global affairs in profound ways, redefining traditional power dynamics, state authority, sovereignty, security and foreign policy influence. They wield economic and security power that rivals nation states, enabling them to impact international trade, communications, warfare and even political processes.

Moreover, Big Tech's investments in EDTs like AI, quantum computing, semiconductors and biotechnologies, among others, position them as key players in the future of technological innovation, and hence in the future of humanity. Their ability to outspend most countries on the research and development of EDTs means they are at the vanguard of technological advances, driving global standards and practices in all fields. Their global reach and resources enable them to lobby effectively, shaping regulatory environments to suit their interests and often surpassing the influence of smaller nations. As a result, traditional international relations power structures are being disrupted, with Big Tech firms acting as quasi-sovereign entities on the global stage. This new dynamic necessitates a rethinking of global governance and foreign policy to address states' increasing sovereignty gap in comparison with tech giants, and the growing influence of these corporate players wielding the disruptive effects of EDTs in all aspects of society, economy, politics and security.

Dr. Raluca Csernatoni

Research Fellow at Carnegie Europe and Professor with the Centre for Security, Diplomacy and Strategy (CSDS) at the Vrije Universiteit Brussel's (VUB) Brussels School of Governance

Dr. Raluca Csernatoni is a research fellow working on European security and new technologies like Artificial Intelligence (AI) at Carnegie Europe in Brussels, Belgium. At Carnegie, she is a team leader and senior expert on new technologies for the 'EU Cyber

Diplomacy Initiative - EU Cyber Direct' (EUCD) project and leads Carnegie Europe's research project on 'The EU's Techno-Politics of AI' supported by the McGovern AI Grant. Csernatoni is currently also a professor on European security and defence focusing on emerging and disruptive technologies at the Brussels School of Governance (BSoG) and its Centre for Security, Diplomacy and Strategy (CSDS), Vrije Universiteit Brussel (VUB), Belgium. At CSDS, she is a senior research expert on digital technologies in the context of the EU-funded project, 'Indo-Pacific-European Hub for Digital Partnerships: Trusted Digital Technologies for Sustainable Well-Being - INPACE'. Additionally, Csernatoni is a visiting professor of European security and high-tech warfare with the Department of International Relations of Central European University (CEU) in Vienna, Austria.

Select Bibliography

Taylor Rajik and Julia Brock

Cyber diplomacy

Barrinha, André, and Thomas Renard, 'Cyber-Diplomacy: The Making of an International Society in the Digital Age.' *Global Affairs* 3 (4–5): 353–64. 2017.

Barrinha, André, and Thomas Renard, 'The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyberspace', *Council on Foreign Relations*, 2020. https://www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace

Barrinha, André, 'Cyber-diplomacy: The Emergence of a Transient Field', *The Hague Journal of Diplomacy* (published online ahead of print, 2024), doi: https://doi.org/10.1163/1871191x-bja10183

Basu, Arindrajit, and Karthik Nachiappan, 'Will India Negotiate?', in *Hybridity, Conflict, and the Global Politics of Cybersecurity*, ed. Fabio Cristiano and Bibi van den Berg (Lanham, MD: Rowman & Littlefield, 2023), p. 189.

Buchanan, Ben, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Oxford: Oxford University Press, 2017).

Carr, Madeline, 'Cyberspace and International Order', in *The Anarchical Society at 40: Contemporary Challenges and Prospects*, ed. Hidemi Suganami, Madeline Carr and Adam Humphreys (Oxford: Oxford Academic, 2017).

Christou, George, 'Cyber Diplomacy: From Concept to Practice', *Tallin Papers,* 2024, 1–14. https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf

Clarke, Richard A., 'Securing Cyberspace through International Norms: Recommendations for Policymakers and the Private Sector,' Good Harbor Security Risk Management, 2012. https://carnegie-production-assets.s3.amazonaws.com/static/files/Good-Harbor_Securing-Cyberspace-Through-International-Norms_2013.pdf

Clarke, Richard A., and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2012).

Deibert, Ron, 'Bounding Cyber Power: Escalation and Restraint in Global Cyberspace', Internet Governance Papers: Paper No. 6, Center for International Governance Innovation, October 2013. https://www.cigionline.org/sites/default/files/no6_2.pdf

Goldman, Emily O., 'From Reaction to Action: Revamping Diplomacy for Strategic Cyber Competition', *Texas National Security Review*, vol. 3, no. 4 (2023), 153–76.

Healey, Jason, 'Pursuing Cyber Statecraft', Atlantic Council, 2011. http://www.jstor.org/stable/resrep03355.

Healey, Jason (ed.) A Fierce Domain: Conflict in Cyberspace 1986–2012 (Vienna, VA: Cyber Conflict Studies Association, 2013).

Hogeveen, Bart, Arindrajit Basu, Isha Suri and Baani Grewal, 'Negotiating Technical Standards for Artificial Intelligence: A Techdiplomacy Playbook for Policymakers and Technologists in the Indo-Pacific' (2024). https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2024-06/Negotiating%20technical%20standards%20for%20artificial%20intelligence.pdf

Hurel, Louise Marie, 'The Political Cybersecurity Blindfold in Latin America', *Default*, 26 April 2023. https://www.lawfaremedia.org/article/the-political-cybersecurity-blindfold-in-latin-america/

Johnstone, Ian, Arun Mohan Sukumar and Joel P. Trachtman. *Building an International Cybersecurity Regime: Multistakeholder Diplomacy* (Cheltenham: Edward Elgar, 2023).

Kaplan, Fred M., *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2017).

Kello, Lucas, 'Digital Diplomacy and Cyber Defence', in *The Oxford Handbook of Digital Diplomacy*, ed. Corneliu Bjola and Ilan Manor (Oxford: Oxford Academic, 2024).

Klimburg, Alexander, and Heli Tiirmaa-Klaar, 'Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU', European Parliament, Directorate-General for External Policies of the Union, April 2011. https://www.europarl.europa.eu/thinktank/en/document/EXPO-SEDE_ET(2011)433828

Lewis, James A., 'Multilateral Agreements to Constrain Cyberconflict', *Arms Control Today*, 2010. https://www.armscontrol.org/act/2010-06/multilateral-agreements-constrain-cyberconflict

Lewis, James A., 'Creating Accountability for Global Cyber Norms', CSIS, 2022. https://www.csis.org/analysis/creating-accountability-global-cyber-norms

Lilli, Eugenio, and Christopher Painter, 'Soft Power and Cyber Security: The Evolution of US Cyber Diplomacy', in *Soft Power and the Future of US Foreign Policy*, ed. Hendrik W. Ohnesorge (Manchester: Manchester University Press, 2023), pp. 161–79.

Lonergan, Erica D., and Shawn W. Lonergan, *Escalation Dynamics in Cyberspace* (New York: Oxford Academic, 2023).

Manantan, Mark Bryan, 'Advancing Cyber Diplomacy in the Asia Pacific: Japan and Australia', *Australian Journal of International Affairs*, vol. 75, no. 4 (2021), pp. 432–59.

Neutze, Jan, and J. Paul Nicholas, 'Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cyber Security

Norms', *Georgetown Journal of International Affairs*, 2013, 3–15. http://www.jstor.org/stable/43134318.

Painter, Chris, 'Diplomacy in Cyberspace', *Foreign Service Journal*, June 2018, https://www.afsa.org/diplomacy-cyberspace

Pavel, Tal, 'Israel's Cyber Diplomacy – Looking for Israel's Cyber Ambassador', *Diplomacy & Intelligence / Revistă de Științe Sociale, Diplomație și Studii de Securitate*, 2020. https://www.ceeol.com/search/article-detail?id=879290

Public Diplomacy, 'Cyber Diplomacy', issue 22, winter 2019. https://publicdiplomacy.org/docs/CyberDiplomacy+Magazine.pdf

Raymond, Mark, and Justin Sherman, 'Authoritarian Multilateralism in the Global Cyber Regime Complex: The Double Transformation of an International Diplomatic Practice', *Contemporary Security Policy*, vol. 45, no. 1 (2023), 110–40.

Riordan, Shaun, *Cyberdiplomacy: Managing Security and Governance Online* (Cambridge: Polity, 2019).

Segal, Adam, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: PublicAffairs, 2017).

Sukumar, Arun, Dennis Broeders and Monica Kello, 'The Pervasive Informality of the International Cybersecurity Regime: Geopolitics, Non-State Actors and Diplomacy', *Contemporary Security Policy*, vol. 45, no. 1 (2024), 7–44.

Tiirmaa-Klaar, Heli, 'Cyber Diplomacy: Agenda, Challenges and Mission', *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 509–31.

Tiirmaa-Klaar, Heli "Cyber Diplomacy", in Kralev, N. (Ed.) *Diplomatic Tradecraft* (Cambridge: Cambridge University Press, 2024).

https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ce94c6084857b1649b1748bf5210025fd77011fa#page=544

International cyber law

Biller, Jeffrey T., and Michael N. Schmitt. 'Classification of Cyber Capabilities and Operations as Weapons, Means or Methods of Warfare', *International Law Studies*, vol. 95 (2019), pp. 179–225.

Broeders, Dennis, Els de Busser, Fabio Cristiano and Tatiana Tropina, 'Revisiting Past Cyber Operations in Light of New Cyber Norms and Interpretations of International Law: Inching towards Lines in the Sand?', *Journal of Cyber Policy*, vol. 7, no. 1 (2022), pp. 97–135.

Chertoff, Michael, and Paul Rosenzweig, 'A Primer on Globally Harmonizing Internet Jurisdiction and Regulations', Global Commission on Internet Governance, Paper Series No. 10, March, Centre for International Governance Innovation (CIGI) and Chatham House, 2015.

Delerue, François, *Cyber Operations and International Law* (Cambridge: Cambridge University Press, 2020).

Finnemore, Martha, and Duncan B. Hollis, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity', *European Journal of International Law* (2020). http://dx.doi.org/10.2139/ssrn.3347958

Hollis, Duncan B., 'A Brief Primer on International Law and Cyberspace', Carnegie Endowment for International Peace, 14 June 2021, https://carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace?lang=en

'International and Foreign Cyberspace Law Research Guide: Treaties & International Agreements on Cyber Crime', Georgetown Law Library, Georgetown Law.

https://guides.ll.georgetown.edu/cyberspace/cyber-crime-treaties

Lewis, James A., 'A Note on the Laws of War in Cyberspace', CSIS, 25 April 2010. https://www.csis.org/analysis/note-laws-war-cyberspace.

Liebetrau, T., 'Cyber Conflict Short of War: A European Strategic Vacuum', *European Security*, vol. 31, no. 4 (2022), pp. 497–516.

Mačák, K., 'Unblurring the Lines: Military Cyber Operations and International Law', *Journal of Cyber Policy*, vol. 6, no. 3 (2021), pp. 411–28. https://doi.org/10.1080/23738871.2021.2014919

Moynihan, Harriet. 'The Application of International Law to State Cyberattacks.' Chatham House, 2019. https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks

Moynihan, Harriet, 'The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace', *Journal of Cyber Policy*, vol. 6, no. 3 (2020), pp. 394–410.

Pijpers, Peter B.M.J., 'Careful What You Wish For: Tackling Legal Uncertainty in Cyberspace', *Nordic Journal of International Law*, vol. 92, no. 3 (2023), pp. 394–421,

Raymond, Mark, 'Applying Old Rules to New Cases: International Law in the Cyber Domain', paper presented to the International Studies Association, Atlanta, GA, 16–19 March 2016.

Solis, Gary D., 'Cyber in the Law of Armed Conflict', in *The Law of Armed Conflict: International Humanitarian Law in War* (Cambridge: Cambridge University Press, 2021) pp. 532–61.

Taillat, Stéphane, 'Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security', *Contemporary Security Policy*, vol. 40, no. 3 (2019), pp. 368–81.

Walker, Clive, and Ummi Hani Binti Masood, 'Domestic Law Responses to Transnational Cyberattacks and Other Online Harms: Internet Dreams Turned to Internet Nightmares and Back Again', *Notre Dame Journal of International & Comparative*

Law, vol. 10, no. 1 (2020), article 6. https://scholarship.law.nd.edu/ndjicl/vol10/iss1/6

As cyberspace becomes a central domain of international relations, diplomacy must evolve to meet new challenges and opportunities. **A Handbook for the Practice of Cyber Diplomacy** provides a clear and practical guide to how diplomacy is adapting in the digital age. Edited by Andrea Salvi, Heli Tiirmaa-Klaar, and James Andrew Lewis, this volume brings together seasoned diplomats and practitioners to explore the emerging area of cyber diplomacy.

Through more than 20 essays, the book examines multilateral and regional efforts, national perspectives, and key issues such as international law, norms of responsible state behaviour, capacity building, and the role of emerging technologies. Rather than focusing on technical cybersecurity, it highlights the diplomatic skills, strategies, and policies needed to navigate this complex and fast-moving field.

Designed for diplomats, policymakers, and experts working at the intersection of technology and international affairs, this handbook offers essential insights for shaping a stable, secure, and cooperative digital environment.

EU CYBER DIRECT

IMPLEMENTING ORGANISATIONS

euiss European Union Institute for Security Studies

CARNEGIE EUROPE

FUNDED BY THE EUROPEAN UNION

Publications Office of the European Union

ISBN 978-92-9462-513-7
CATALOGUE NUMBER QN-01-25-071-EN-N