

**Agnieszka Wierzbicka** is an expert on Cyber Security, International Relations and Media. She has worked in the Polish and German administration for more than 14 years, advising five Speakers of the Polish Parliament, the Polish and German President as well as Deputy Minister of Digital Affairs and Plenipotentiary to the Polish Government for Cyber Security. Ms. Wierzbicka is currently a National Expert delegated to Security and Defence Policy Division, Cybersecurity Sector at the European Union External Action Service in Brussels and her focus is on cybersecurity of the emerging and disruptive technologies, cybercrime, resilience and Africa. She was involved in the implementation process of the NIS Directive and is co-author of the Polish first cyber security strategy. She is also an expert of the Technical Assistance and Information Exchange (TAIEX) instrument of the European Commission with the goal to support public administrations with regard to the approximation, application and enforcement of EU legislation as well as facilitating the sharing of EU best practices.

**Alexandra Paulus** is Non-Resident Fellow for International Cyber Security Policy at Berlin tech policy think tank Stiftung Neue Verantwortung and pursues her PhD in International Relations at Chemnitz University of Technology in Germany. Her research explores how states shape the construction of norms for responsible state behavior in cyberspace, focusing on Brazil. Alexandra is an active member of the Konrad Adenauer Foundation's Working Group of Young Foreign Policy Experts and of Women in International Security Germany (WIIS.de). Before commencing her doctoral degree, Alexandra was deputy head of the Konrad Adenauer Foundation Brazil office.

**Aman Nair** is a policy officer under the Cybersecurity and Data Governance project at the Centre for Internet and Society, India. His current research is focused on the relationship between digital infrastructure, governance and rights - specifically the impact of technology on judicial infrastructure. His previous research was on the impact of Indian Soft Power globally and has developed and published a report on how to identify and quantify soft power in a foreign state. He holds a Humanities Degree from Sciences Po, Paris with a major in Economics.

**Amy Ertan** is a Cyber Security Doctoral Candidate at Royal Holloway, University of London. Her research explores the security implications of emerging technologies within the military and defence environments. Amy is a research fellow at the Harvard Kennedy School's Belfer Center and is a visiting scholar at the NATO Cooperative Cyber Defence Center of Excellence. Amy is also a Data Protection Fellow at the Institute for Technology and Society, Rio de Janeiro, where she has lectured on oversight mechanisms for AI-enabled technology. Amy has previously worked for a number of years as a strategic cyber intelligence analyst within a large financial institution. She has a Bachelor's degree in Philosophy, Politics and Economics from the University of Oxford.

**Anastasiya Kazakova** is a Public Affairs Manager at Kaspersky. In this role, Anastasiya coordinates the company's worldwide public policy with a focus on cyber diplomacy/global

projects, and the Global Transparency Initiative – Kaspersky's program to enhance transparency and accountability in cybersecurity.

**Anjali Kaushik** is a Professor at Management Development Institute (MDI), Gurgaon which is a premier B-School in India. At MDI, Gurgaon she is also the Chair for the Centre on Cyber Security. Apart from being a PhD in information systems, she also has a Post-graduate Diploma in Cyber Law & Cyber Forensics from National Law School of India University, Bangalore. She is empanelled as Lead Expert on Cyber Security with Government of India and was also the Principal Investigator for the project to deliver the Information Security Assurance Framework with Ministry of Communication and IT, Government of India. She is a regular speaker and panelist on cyber security and privacy related themes at various forums and has been a part of the delegation on Cyber Dialogue with Indian government to multiple countries. She has written two books and several journal articles on cyber security, privacy and data protection.

**Anriette Esterhuysen** was the executive director of APC until March 2017. Prior to joining APC, Anriette was executive director of SANGONeT, an internet service provider and training institution for civil society, labour and community organisations. She was active in the struggle against Apartheid from 1980 onwards. From 1987 to 1992 she did information and communication work in development and human rights organisations in South Africa and Zimbabwe. Anriette, with many others, helped establish email and internet connectivity in Southern Africa. SANGONeT hosted a Fidonet hub that provided universities and non-governmental organisations in, among other places, Malawi, Zambia and Zimbabwe, with email links to global networks as part of a collaboration between APC and the United Nations Development Programme. Anriette has served on the African Technical Advisory Committee of the UN's Economic Commission for Africa's African Information Society Initiative and was a member of the United Nations ICT Task Force from 2002 to 2005, the World Summit on the Information Society (WSIS) Working Group on Financing Mechanisms, and the Commission on Science and Technology for Development Working Group on Internet Governance Forum (IGF) Improvements. She was a member of the Multistakeholder Advisory Group of the Internet Governance Forum from 2012 to 2014. Anriette was one of five finalists for IT Personality of the Year in South Africa in 2012, an award which recognises a person who has made an outstanding impact on the South African ICT industry. She was the only female and only civil society finalist. She was inducted into the Internet Hall of Fame as a Global Connector in 2013. Currently Anriette is a member of the Global Commission on Internet Governance and the Council of the NETmundial Initiative. She has published extensively on ICTs for development and social justice. She holds a BA in social sciences and postgraduate qualifications in history of music and information sciences from the University of the Witwatersrand in Johannesburg, South Africa.

**Arindrajit Basu** is a research manager at the Centre for Internet & Society, India, where he focuses on the geopolitics and constitutionality of emerging technologies. He is a lawyer by training and holds a BA, LLB (Hons) degree from the National University of Juridical

Sciences, Kolkata, and an LLM in public international law from the University of Cambridge, U.K.

**Beatriz Kira** is a Senior Research and Policy Officer at the Blavatnik School of Policy, University of Oxford, working on a project about governance of digital technologies in developing countries (Digital Pathways at Oxford). Beatriz is a lawyer by training and has earned a Master in Social Science of the Internet from the Oxford Internet Institute. She is currently pursuing her PhD in Economic Law at the University of São Paulo.

**Bruna Toso de Alcântara** is a PhD candidate in the Graduate Program in International Strategic Studies (PPGEEI) at the Federal University of Rio Grande do Sul (UFRGS) and a research fellow at the Alexander von Humboldt Institute for Internet and Society (HIIG). She holds a Master's in International Strategic Studies from UFRGS and a bachelor degree in International Relations from the Federal University of Santa Maria (UFSM). Her research interests are Cybersecurity, Cyberdefense, Technology, State and International Security, and International Strategic Studies.

**Caitríona Heint** is Executive Director at The Azure Forum for Contemporary Security Strategy, Ireland and Adjunct Research Fellow at the School of Politics and International Relations at University College Dublin. Caitríona has over a decade of experience in international and Irish research and academic environments working on transnational crime, security and defence questions with particular focus on international cybersecurity policy, emerging technologies, and regional security architectures. Her work has included research, projects and lectures at home and abroad for government agencies, international organisations and industry such as the UN, NATO, the OSCE, the EU, ASEAN/ARF, military colleges, ministries of defence, the Irish government's Departments of Justice and Defence, cybersecurity corporations and insurance companies. Caitríona was previously responsible for policy under the NTU Cyber Risk Management project, having transferred from the S. Rajaratnam School of International Studies (RSIS) Centre of Excellence for National Security at NTU Singapore where she worked as Research Fellow on international cybersecurity from 2012 to 2018. In this role, she provided policy analysis to the National Security Coordination Secretariat and other government agencies. She previously led the Justice and Home Affairs policy group and Justice Steering Committee at the Institute of International and European Affairs (IIEA Dublin). She is a member of the Irish government's Department of Foreign Affairs Foreign Policy Network, having held Fellowships with the ASPI International Cyber Policy Centre and Leiden University.

**Cathrin Bauer-Bulst** is acting head of unit for the fight against cybercrime and child sexual abuse in DG Migration and Home Affairs of the European Commission. Her unit develops legislative proposals and policy and coordinates EU efforts in these areas, playing a leading role in the current negotiations of international instruments on cybercrime such as the Second Additional Protocol to the Budapest Convention and the new UN process. She co-chairs the Commission's informal task force on electronic evidence and the Governmental Advisory Committee Working Group on Public Safety issues within ICANN. Cathrin has a background

in law and IT; prior to her career at the Commission, she worked for an international law firm in Brussels and an IT consultancy in New York. She is a fully qualified lawyer trained in Germany and France and also holds a degree in history and literature from Harvard College.

**Christian Perrone** is a Ph.D. Candidate at UERJ and a Fulbright Scholar at the Georgetown Law Center with particular focus on international regulation and technology. He also has a LL.M. in International Law from the University of Cambridge (UK) and a Diploma in International Human Rights Law from the European University Institute. He was the former Secretary for the Inter-American Juridical Committee from the Organization of American States (OAS) collaborating closely with Rapporteur on Privacy and Data Protection. He also worked as a consultant for freedom of expression online in Cuba for Freedom House and as a human rights specialist for the Inter-American Commission on Human Rights and the Inter-American Court of Human Rights. His current interest lies in the intersection of regulation, technology and public policy with special attention towards privacy and data protection.

**Daan Weggemans** is program director of the Bachelor security studies and a researcher at the Institute of Security and Global Affairs (ISGA) at Leiden University/Campus The Hague. He is also a Research Fellow at the International Centre for Counter-Terrorism (ICCT). Earlier research focused on processes of (de)radicalisation and re integration, the radicalisation and preparatory processes of Foreign Fighters and contemporary security technologies. He has been an expert witness in various court cases and interviewed dozens of security professionals and (former) violent extremists and their families.

**Dan McBryde** obtained a Master's degree in history at the University of Ottawa. He then completed a second Master's degree in international relations at Carleton University. Before joining the Canadian civil service in 2006, Dan worked as a history professor and served as a policy advisor to a Member of Parliament and a Senator. Since joining Canada's civil service, he has worked as an analyst on a range of files in several departments, including Afghanistan counter narcotics; critical infrastructure protection; NAFTA and Trans-Pacific Partnership negotiations; and the counter-ISIS campaign. He has also served as a speechwriter to the Minister of National Defence and as a senior analyst supporting the Senate National Security and Defence committee. He is currently a senior policy advisor at Global Affairs Canada's international cyber policy team, where he leads on UN cyber negotiations and norms of state behaviour in cyberspace, among other files. He supported Canada's expert at the 2016-17 UN GGE and is currently the lead officer supporting Canada's expert at the UN OEWG.

**Danielle Kriz** joined Palo Alto Networks in February 2016 as Senior Director of Global Policy. In this position, she leads the company's engagement with governments around the world on cybersecurity and other public policy issues that impact Palo Alto Networks. Danielle has 24 years of technology, cybersecurity, and trade policy experience. She previously was Director for Global Cybersecurity Policy at the Information Technology Industry Council (ITI), a Washington, D.C.-based trade association representing the world's largest technology companies. Prior to ITI, Danielle spent four years in Silicon Valley consulting on government affairs strategies for high-tech and clean-tech firms. She began her career with ten years in

government, working on high-tech trade policies at the U.S. International Trade Commission and then the U.S. Department of Commerce's International Trade Administration, where she spearheaded the U.S. Government's work on cybersecurity as it intersects with trade. Danielle has worked with governments and engaged on cybersecurity policies in the U.S., EU, Japan, the U.K., Singapore, China, India, Korea, Brazil, and many others. Danielle has an MS in Foreign Service from Georgetown University, with a focus on international trade and technology policy, and a BA from Ithaca College in politics. She lived in Tokyo from 1991-1994.

**Dennis Broeders** is Associate Professor of Security and Technology and Senior Fellow of The Hague Program for Cyber Norms at the Institute of Security and Global Affairs of Leiden University, the Netherlands. His research and teaching broadly focuses on the interaction between security, technology and policy, with a specific interest in international cyber security governance. He is the author of the book *The public Core of the Internet* (2015). He currently also serves as a member of the Dutch delegation to the UN Group of Governmental Experts on international information security (2019-2021) as an academic advisor

**Duncan B. Hollis** is Laura H. Carnell Professor of Law at Temple University Law School in Philadelphia. He is editor of the award-winning *Oxford Guide to Treaties* (2012, 2nd ed., 2020) and (with Allen Weiner) *International Law* (2018), one of the leading textbooks in the field. Professor Hollis has authored a series of articles on securing cyberspace, including (with Martha Finnemore) "Constructing Norms for Global Cybersecurity," which was published in the *American Journal of International Law*, and the forthcoming *European Journal of International Law* Article, "Beyond Naming & Shaming: Accusations and International Law in Cyberspace". A former Attorney-Adviser at the U.S. Department of State, Professor Hollis is a Non-Resident Scholar at the Carnegie Endowment for International Peace and a member of the American Law Institute. In 2016, Professor Hollis was elected by the General Assembly of the Organization of the American States to a four year term on the OAS's Inter-American Juridical Committee, where he is the Rapporteur for a project on improving the transparency of how States understand international law applies in cyberspace."

**Edrine Wanyama** is an Advocate of the Courts of Judicature of the Republic of Uganda. He has more than eight years' experience and expertise in advocacy and research in human rights, rule of law and democracy. He holds a Master of Laws (LL.M) from Makerere University-Uganda, a Master of Laws (LL.M) from the University of Dar es Salaam, Tanzania, a Bachelor of Laws Degree (LL.B) from Makerere University and a Diploma in Legal Practice (Dip L.P) from the Law Development Centre (Uganda). Edrine has also undertaken leadership training with the Friedrich Ebert Stiftung Germany Foundation and in digital rights and freedoms with various key players. He is a specialist in East African Community Law, Economic Integration, International Law, Human Rights and associated Mechanisms and the Law governing Not-for-profit Organisations. He has a lecturer at law in a number of universities in Uganda and has written and published widely in social, economic and political legal imperatives. He is currently the Legal Officer of the Collaboration on International ICT Policy for East and

Southern Africa (CIPESA), an organisation focused on facilitating the use of ICTs to support of development, poverty reduction and digital transformation in Africa.

**Eli Sugarman** is Director of the Cyber Initiative at the William and Flora Hewlett Foundation. He leads a ten-year, \$130 million grant-making effort that aims to build a more robust cybersecurity field and improve policy-making. Previously, he was a consultant and strategist to private sector and nonprofit leaders. From 2009 to 2014, Eli was senior director at an emerging markets advisory firm based in Washington, D.C., where he provided strategic counsel on international policy, regulatory, and business matters to clients globally. He has served as a foreign affairs officer at the U.S. Department of State, where he focused on international security issues. Eli also serves on the executive board of the CyberPeace Institute (CPI) and Independent Advisory Committee of the Global Internet Forum to Counter Terrorism (GIFCT). He writes regularly about cybersecurity, government surveillance, data privacy and internet governance in leading outlets. A San Diego native and graduate of Middlebury College, he holds a J.D. from Stanford University Law School.

**Emily Taylor** is an associate fellow with the International Security programme of Chatham House. She is CEO of Oxford Information Labs, author of several research papers, and is a frequent panellist and moderator at conferences and events around the world. Previous roles have included chair of ICANN WHOIS Review Team, Internet Governance Forum Multistakeholder Advisory Group, Global Commission on Internet Governance research network, and director of Legal and Policy for Nominet. She has written for the Guardian, Wired, Ars Technica, the New Statesman and Slate, and has appeared on the BBC Now Show and the BBC Radio 4 'Long View'. Emily is a graduate of Cambridge University, qualified as a solicitor in England and Wales, and has an MBA from the Open University.

**Enrico Calandro** is co-director at the Cybersecurity Capacity Centre for Southern Africa, University of Cape Town (C3SA), and Senior Research Associate at Research ICT Africa. Over the past 10 years, Enrico has been exploring the relationship between digitalisation and development in the African context.

**Eva Claessen** is a PhD researcher in Russia studies at the Leuven Centre for Global Governance Studies (GGG). She holds a Master Slavic and East-European Studies from KU Leuven. In 2016, she started her academic career as a teaching assistant for Slavic and East European Studies, during which time she did research on Russia's Military and Security policy with a focus on Russian perspectives on information warfare. Prior to starting her PhD in 2018, she was an assistant for EU correspondents of various television stations from all over Europe, for whom she provided research and logistical support. Her research interests include Russian foreign and security policy, as well as Russian perspectives on the global governance of cyber space. She is involved in the project *Connectivity*, which offers an assessment of how differences between prominent States' conceptualisation of international norms impact upon cooperation in the international system. In this context, she is working on Russia's role in cyber norm development as well as domestic Internet policy formation. Her PhD thesis titled "Defining virtual borders – the impact of securitizing and civilizational narratives on the

formation of Internet policy by Russia” focuses on the evolution of Russia’s Internet policy both domestically and abroad, as well as the impact strategic narratives have on the way Russia aims to advance its preferred normative framework.

**Fabio Cristiano** is a postdoctoral researcher in the Institute of Security and Global Affairs at Leiden University and fellow of The Hague Program for Cyber Norms. His research and teaching broadly lie at the intersection of critical security studies and IR theory, with a specific interest for automation, autonomy, and normative debates in the international context of cyber and information security. Fabio’s publications have explored a wide array of topics, including national security policies, cyber warfare in Palestine/Israel, digital rights, cyberwar games simulations, augmented reality, cyborg theory, and algorithmic security governance.

**Fabrizio Tassinari** serves as the Executive Director of the School of Transnational Governance, where he develops the overall strategic direction, the design and the policy programme of the School. Between 2009 and 2017, Tassinari served as Senior Researcher and Head of the Foreign Policy Studies unit at the Danish Institute for International Studies. Since 2012, he has also been a Visiting Professor at the Department of Social Science at Humboldt University in Berlin, where he was an awardee of an Alexander von Humboldt fellowship. Tassinari, a political scientist, has a background in research and policy advice on questions of democracy, governance and international security, in and around Europe. He is the author of the book 'Why Europe Fears its Neighbors' (Praeger), which also appeared in an updated Turkish-language edition for the mass market. His writing regularly features in mainstream international media, such as the Economist, the Financial Times, CNN, Foreign Affairs, the Christian Science Monitor, Le Figaro and Die Welt. His academic output has been published in peer-reviewed journals and volumes, including the European Foreign Affairs Review, Mediterranean Politics, the International Spectator and Cooperation and Conflict. Tassinari has advised several Western governments and international organisations; his 2007 policy brief on Black Sea cooperation provided the blueprint and the official name of a European Union policy.

**Farlina Said** is an Analyst in the Foreign Policy and Security Studies programme of ISIS Malaysia since 2015. She graduated from S Rajaratnam School of International Studies (RSIS), Nanyang Technological University with a MSc (Strategic Studies). As a part of the think tank she was involved in crafting various dialogues and forums on cybersecurity, radicalisation and Malaysia-Korea relations. Her written work and comments have appeared in local, regional and international media such as *New Straits Times*, *the Nation* (Thailand), *China Daily*, *CGTN* and *South China Morning Post*. She is active in networks, inclusive of the Council for Security Cooperation in the Asia Pacific (CSCAP) where she had constructed discussions in the Malaysian-leg of the CSCAP Study Group on International Law and Cyberspace. She was also appointed to be a part of SEARCCT’s Experts on Violent Extremism and Community Engagement (EVOKE) Council (2018-2019) and had participated in the ROK Ministry of Unification Institute for Unification Education (IUE) Emerging Leaders Fellowship in 2019.

**Francesca Bosco** is Senior Advisor on Capacity Building and Foresight at the CyberPeace Institute. She has an academic background in International Law and Human Rights, and joined the United Nations in 2006, working on action oriented research, capacity building and technical assistance in the areas of international justice, crime and security. She has developed her expertise on cybercrime, cybersecurity and misuse of technology, in recent years focusing on opportunities, risks and threats created by new technologies. She then joined the Center for Cybersecurity of the World Economic Forum working on cyber resilience and public policy initiatives, collaborating with a wide multi-stakeholder network of partners to improve the state of global cybersecurity, focusing on building cyber capabilities. In her current role, she is leading the creation and dissemination of knowledge and initiatives on how emerging and disruptive technologies are affecting societies, and how to increase resilience through capacity building in order to foster responsible behavior in cyberspace and create and maintain cyberpeace.

**François Delerue** is currently research fellow in cyberdefense and international law at the Institute for Strategic Research (Institut de Recherche Stratégique de l'École Militaire – IRSEM) and an adjunct lecturer at Sciences Po Paris. François is also rapporteur for international law in the EU Cyber Direct project. He just published his book titled 'Cyber Operations and International Law' with CUP. François' research concerns cyberdefense and cybersecurity, specifically their legal, policy and strategic dimensions. His research focuses on international law obligations, norms and international cooperation, as well as on the various actors involved in this area, including States, private companies, non-governmental organisations. More broadly, he is interested in how new technologies and activities (space activities, cyber, robotics and artificial intelligence) challenge international law and international relations. François regularly lectures at the International Institute for Humanitarian Law at Sanremo (Italy) and in the Master in Cybersecurity of the Military Academy of Saint-Cyr (France). He has taught at the European University Institute (EUI), Sciences Po Paris and the University of Florence (Università degli Studi di Firenze). He is frequently invited to present at conferences and give guest lectures domestically and internationally. He was previously a visiting researcher at Columbia University in New York and a Young Scholar Fellow at the Global Relations (Global İlişkiler Forumu) in Istanbul. He defended his PhD on cyber operations and international law in November 2016 at the EUI, Florence, Italy. His doctoral research, conducted under the supervision of Professor Nehal Bhuta, was sponsored by the IHEDN, the IRSEM and the French Ministry of Research and Higher Education. He graduated with a Masters in international law and international organizations from the Sorbonne Law School (Paris 1 University). He holds an LLM in Comparative, European and International Laws from the EUI. He attended the 62nd youth seminar of the IHEDN (2009) and the international law and cyber operations seminar of the NATO School in Oberammergau (2013).

**Frédéric Douzet** is a Professor at the French Institute of Geopolitics at Paris 8 University and has been chairwoman of the Castex Chair of Cyber Strategy since February 2013. Her current research deals with the geopolitics of cyberspace. She manages a multidisciplinary team of graduate students at the University of Paris 8 and the Castex Chair of Cyberstrategy

and covers a wide range of topics. She studied political science at the Institute of Political Studies of Grenoble and Oxford Brookes University. She earned a Master's degree from the Graduate School of Journalism at UC Berkeley in 1993 then joined the graduate school of geopolitics at the University of Paris 8. She has been a member of the editorial board of the review *Hérodote* since 1994.

**Gbenga Sesan** is the Executive Director of Paradigm Initiative, a pan-African social enterprise working on digital inclusion and digital rights through its offices in Cameroon, Ghana, Kenya, Nigeria, Tanzania and Zambia. He is also a Non-Resident Fellow at the Digital Civil Society Lab at Stanford University. Prior to starting Paradigm Initiative, 'Gbenga led the Lagos Digital Village, a joint project of Junior Achievement of Nigeria, Microsoft and Lagos State Government. Originally trained as an Electronic & Electrical Engineer at Obafemi Awolowo University, he completed Executive Education programs at Lagos Business School, New York Group for Technology Transfer, Oxford University, Harvard University, Stanford University, Santa Clara University and University of the Pacific. 'Gbenga's consulting experience includes assignments completed for numerous institutions, including Microsoft, Harvard University and United Nations agencies, among others, in over 35 countries. A Schwab Foundation Social Entrepreneur of the Year and former member of the United Nations Committee of eLeaders on Youth and ICT, he is a CyberStewards Fellow, Crans Montana Forum Fellow, Archbishop Desmond Tutu Leadership Fellow, Ashoka Fellow, Our Common Future Fellow and Cordes Fellow. 'Gbenga served as a member of the Presidential committees on Harmonization of Information Technology, Telecommunications and Broadcasting Sectors (2006) and Roadmap for the Achievement of Accelerated Universal Broadband Infrastructure and Services Provision (2013), and was listed by CNN as one of the Top 10 African Tech Voices on Twitter and by Ventures Africa as one of 40 African Legends Under 40. 'Gbenga is married to Temilade Sesan, PhD, an expert on Energy Poverty and Development. He has been advising the World Health Organisation on Data Privacy during the ongoing pandemic and is also advising the World Economic Forum on its Operationalising Trust Project, to develop rights-respecting Data Policy for businesses.

**George Christou** has been at the University of Warwick, UK since 2005 where he is now Professor of European Politics and Security. He has published widely on European Politics and Security and participated in a number of EU, NATO-ACT and UK-funded security-related projects over the past fifteen years and EU platforms relating to cybersecurity and Internet Governance. He has published in journals such as *Governance*, *Journal of Public Policy*, *Journal of European Integration*, *Journal of European Public Policy*, *Journal of Common Market Studies*, *Political Geography*, *European Security and Cooperation and Conflict*. He is the Editor for Palgrave's *New Security Challenges Series* and his own books include: *Global Standard Setting in Internet Governance*, (Oxford University Press, 2020 with Alison Harcourt and Seamus Simpson) *The European Union and Cybersecurity: Adaptation and Resilience in Governance Policy* (Palgrave Macmillan, 2016); 'European Security Governance' (Routledge, 2012 edited with Stuart Croft); 'The New Electronic Market Place: European Governance Strategies in a Globalising Economy' (Edward Elgar, 2007, with S Simpson); 'The European Union and Enlargement: The Case of Cyprus', (Palgrave, 2004). His latest articles include:

‘The Collective Securitisation of Cyberspace in the European Union’ (2018, West European Politics); ‘The Challenges of Cybercrime in the European Union’ (2018, published in the Journal European Politics and Society)

**Gills Vilar Lopes** is currently a Lecturer in International Relations at the Graduate Program in Aerospace Sciences (PPGCA) at the Brazilian Air Force University (UNIFA) in Rio de Janeiro, and researcher at: RedeCTIDC/Pró-Defesa IV (CAPES/Brazilian Ministry of Defence), GEDAI/UNIFA, GEESI/UFPB and NEPI/UFPE. He has a BA in International Relations from Paraíba State University (UEPB), Brazil, an MA (Hons) and PhD in Political Science from Federal University of Pernambuco (UFPE), Brazil, and a Specialized Course in Cybersecurity: Issues in National and International Security from National Defence University (NDU), Washington DC. His research looks at the intersection of international security issues with cybersecurity and Aerospace Power.

**Graciela Selaimen** is a senior program officer in the Brazil office. She is a journalist, specializing in gender and local development, and has been working for more than 20 years in the areas of digital technologies, communication, human rights, and social justice. At Ford, she has developed strategies and programs in the areas of Technology and Society, Creativity and Freedom of Expression, and Thriving Civic Space, crosscutting gender and race perspectives. Her work has contributed to consolidating the field of digital rights in Brazil and to supporting greater collaboration between organizations in the field of digital technologies, investigative journalism, and culture with organizations and social movements working on human rights and social and environmental justice. Prior to joining Ford in 2013, she was a co-founder and director of the Nupef Institute, a research and advocacy organization on digital rights and internet governance, whose work influences national and international policy and debate. From 2008 to 2013, Graciela was a member of the Multistakeholder Advisory Group of the United Nations Internet Governance Forum. During the same period, she was editor in chief of the *poliTICs* magazine, the first and most influential publication dedicated to digital politics and rights in Brazil. Graciela is certified in dialogues and groups facilitation and is the author of articles and book chapters in the areas of philanthropy, gender and technology, digital rights, surveillance technologies, and protection of activism. She holds a master’s degree in communication and culture from the Federal University of Rio de Janeiro.

**Hannes Ebert** is a Cyber-dialogue Project Officer at the Geneva-based Centre for Humanitarian Dialogue. He also serves as Senior Advisor in the EU Cyber Direct at the German Marshall Fund in Washington DC, focusing on cyber security and diplomacy in Brazil, India and South Korea. Between 2010 and 2018, he served as Research Fellow with the GIGA German Institute of Global and Area Studies, where he conducted research on dispute management, asymmetric warfare and cyber conflicts with a focus on South Asia, and spent multiple visiting fellowships at think tanks in Islamabad and New Delhi. In 2013/14 and 2015, he was seconded to the German Foreign Office’s Policy Planning Staff and Political Directorate for advisory work on strategic engagement with fragile states, rising non-Western powers and the Indian Ocean region. Hannes studied international law and politics in Berlin and Geneva and was a Hölderlin Fellow at the London School of Economics, where he received

his MSc. He obtained a Ph.D. in political science, focusing on territorial conflict behavior in the Indo-Pakistani rivalry, from Hamburg University, and was a visiting fellow at Oxford University's Center for International Studies in 2013 and a postdoctoral fellow at Yale University's MacMillan Center in 2017.

**Heli Tiirmaa-Klaar** is Ambassador-at Large for Cyber Diplomacy at the Estonian Ministry of Foreign Affairs. She started her work in Tallinn in September 2018 as Estonia's first Cyber Ambassador. With two decades of experience in international security and cybersecurity, Ambassador Tiirmaa-Klaar has a proven track record of visionary leadership, excellent communication and management skills, an ability to manage multi-cultural teams and build consensus. Before returning to Tallinn, Ambassador Tiirmaa-Klaar was Head of Cyber Policy Coordination at the European External Action Service (EEAS) between January 2012 and August 2018. When creating the cyber coordination structure in the EEAS, her priority was to develop effective cooperation mechanisms between the 28 EU member states as well as to design and steer the development of the EU's cyber security strategy and of the EU's international cyber policy. In 2013 and 2017 she was responsible for both developing the cybersecurity strategies of the European Union and for the implementation of the EU Cyber Defence Policy Framework. One of the major priorities of Ambassador Tiirmaa-Klaar's work at the EEAS was to kick-start extensive EU capacity building programmes in third countries, with a focus on the fight against cybercrime and emerging cyber threats. This has allowed her to gain a global reach and develop a thorough understanding of key cyber challenges. She was also in the lead for developing the Framework of Joint EU Diplomatic Response to Malicious Cyber Activities. Ambassador Tiirmaa-Klaar joined the Estonian civil service in 1995 and has held various managerial positions in national security fields. Between 2007 and 2010 she worked as the National Cyber Coordinator, developing the world's first whole-of-government cybersecurity strategy and reorganizing the government structures to adequately address cyber issues. Shortly before joining the EEAS, she worked as a Cyber Security Policy Adviser to NATO where she drafted and negotiated the first comprehensive NATO Cyber Defence Policy in 2011. Ambassador Tiirmaa-Klaar holds a Master's degree in International Relations and Political Science. She was a Fulbright Scholar at George Washington University in 1998-1999. Between 2004 and 2006, she held an academic position as the Head of the International Studies Department at Tallinn University, where she set up the academic department and graduate programs on International Studies.

**Hilde Hardeman** is Head of the European Commission's Service for Foreign Policy Instruments (FPI) since 2017. Hilde has spent twenty-five years working for the European Commission, covering external relations and economic and competitiveness issues. From 2014 to 2017, she served as Deputy Head of Cabinet to then Vice-President Katainen in charge of Jobs, Growth, Investment and Competitiveness. Between 2011 and 2014, she was in charge of briefing the President of the Commission for meetings with EU Heads of State or Government. Previously, she headed the Commission's Units for Relations with Russia and with Ukraine, Moldova and Belarus. Becoming Head of the Service for Foreign Policy Instruments in May 2017, she returned to the field of external relations, leading a service with over 200 staff, including 90 colleagues in EU Delegations around the world. Her focus in the service is on

putting the EU's Foreign Policy Instruments to the best possible use in achieving the EU's foreign policy objectives and projecting EU interests abroad. Hilde holds a PhD in Slavic Philology and History of the University of Leuven after studies at Leuven, Stanford University, Paris, Moscow and Amsterdam. She was visiting professor at the College of Europe, and taught History of the Soviet Union and Eastern Europe at Vesalius College, Brussels. She published on Russian history and minority right issues.

**Iлина Georgieva** (LL.M.) is a Medior Research Scientist Integrator at TNO's Strategy and Policy Department since February 2020. As part of the sub-division 'Digital Society', she is currently contributing to projects on responsible data science, wellbeing in policy-making processes, and to a TNO-wide AI mapping exercise. Iлина is also a PhD candidate of The Hague Program for Cyber Norms at Leiden University, focusing in her research on the capacity of intelligence agencies to propagate cyber norms by means of their conduct in cyberspace. Prior to joining TNO, Iлина served as a researcher on the Sweetie Project at eLaw, the Center for Law and Digital Technologies at Leiden University. Her research encompassed a comparative legal study concerning the trans-border investigation of Internet sexual crimes against children. While at eLaw, she also co-authored a comparative study on data protection policies in eight different EU jurisdictions. She also served as a Senior Research Associate and later on as a Counsel for the Public International Law and Policy Group (PILPG) from September 2014 to October 2016. Iлина is an alumna of Utrecht University, where she completed her graduate degree (cum laude) and specialized in Conflict, Security and Human Rights. Previous to that she studied at Heidelberg University, Germany, where she focused on Public International Law, and at the University of Barcelona, from where she holds an introductory degree in Spanish Law.

**Ivar Hartmann** is a Professor at FGV Law School in Rio de Janeiro (bachelors, masters, doctorate), where he has taught Cyberlaw, Regulation of New Technologies, Legal Data Science, Research Methodology and, since 2014, an innovative course called Programming for Lawyers. He coordinates the Center for Technology and Society (CTS-FGV) and the Legal Data Science Nucleus. Ivar's research interests and publications cover topics of Constitutional and Cyberlaw, as well as Empirical Legal Research. Ivar holds an MSc from the Catholic University of Rio Grande do Sul, Brazil, an LL.M. from Harvard Law School and an S.J.D. from the State University of Rio de Janeiro.

**Jakob Bund** is the project lead for the cyber defense project at the Center for Security Studies at ETH Zurich. In this capacity, he is working closely with the Swiss Ministry of Defense to inform policy perspectives on security challenges linked to information technology. Jakob is a fellow for the Transatlantic Digital Debates initiative, which seeks to advance US European engagement on the broader societal implications of digital transformation processes. Previously, he served as research associate at Oxford University's Global Cyber Security Capacity Centre (GCSCC), where he consulted closely with governments, civil society and the private sector to support the inclusive development of cybersecurity strategies. Before joining the GCSCC, Jakob worked as associate analyst at the European Union Institute for Security Studies, where he co-coordinated the Chinese Future Task Force that assessed the international

implications of China's military modernization and industrial policies. In this role, he assisted in preparing the technology and security policy sections of informal diplomatic dialogues between the EU and China. Earlier, Jakob completed research assignments at the Center for Strategic and International Studies, the Foreign Policy Institute at Johns Hopkins University, and the Peace Research Institute Frankfurt, working on issues at the interface of technology and policy-making.

**Jan Martin Lemnitzer** is teaching Cyber Security at the Department of Digitalization at Copenhagen Business School. He was formerly Assistant Professor at the Center for War Studies, University of Southern Denmark, Director of Studies at the Changing Character of War programme, Oxford University and taught at Pembroke College and Christ Church, Oxford. He holds a PhD from the London School of Economics and has published widely on the emergence of global norms from the middle of the 19<sup>th</sup> century until today. He was co-organiser of the 2018 Odense Cyber Security conference (together with the ECFR) funded by the Danish Tech Ambassador and researches the emergence of cyber norms, the question of neutrality and due diligence in cyber space, the potential of cyber security insurance and the ways in which company IT security is measured.

**Jayadev Parida** is a Assistant Professor-I at Amity Institute of International Studies, Amity University, Noida 125. He teaches IR, AI, Geopolitics and research on cyber security and data protection issues.

**Jeroen van der Ham** is associate professor of Cyber Security Incident Response in the Design and Analysis of Communication Systems (DACs) group at the University of Twente. Jeroen combines this with his work at the National Cyber Security Centre in The Netherlands (NCSC-NL). At NCSC-NL he focuses on the many developments in coordinated vulnerability disclosure and ethics of the security profession. At the University of Twente he focuses on incident response, ethics of incident response and internet security research, denial of service attacks, and anonymization in network measurements. Jeroen is an active volunteer for FIRST where, amongst other things, he co-chairs the Ethics SIG.

**Joanna Świątkowska** is an Assistant Professor at AGH University of Science and Technology, where she is engaged in developing AGH's Cybersecurity Center. She is also a co-initiator and lecturer of AGH's first cybersecurity bachelor studies. Initiator and former Programme Director (2014-2019) of the European Cybersecurity Forum – CYBERSEC. Listed among the 100 Eastern Europe's emerging technology stars by the Financial Times & New Europe 100 for 2017 and among the Top 20 Women in Cybersecurity by the Women in Tech summit for 2019. As a recognized cybersecurity expert and speaker, she has been involved in numerous national and international initiatives at the intersection of new technologies and public policies. Among others, she was a member of the Advisory Group for Cybersecurity of the Republic of Poland working within the Polish Presidential National Bureau of Security (2016-2017). Author of numerous articles, reports, and analyses concerning cybersecurity, Joanna is also

the initiator and Chief Editor (2015-2017) of the European Cybersecurity Journal, a public policy-oriented journal concentrated on digital affairs. In 2016 she took part in the U.S. Department of State's International Visitor Leadership Programme (IVLP) on Cybersecurity and Government Interoperability.

**Joe Burton** is a Marie Curie Fellow at Universite libre de Bruxelles, completing the two-year European Commission funded project *Strategic Cultures of Cyber Warfare* (CYBERCULT). He is Senior Lecturer, New Zealand Institute for Security and Crime Science. Joe holds a Doctorate in International Relations and a Master of International Studies degree from the University of Otago and an undergraduate degree in International Relations from the University of Wales, Aberystwyth. He is recipient of the US Department of State SUSI Fellowship, the Taiwan Fellowship, and has been visiting researcher at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, Estonia. Joe is the author of *NATO's Durability in a Post-Cold War World* (SUNY Press, 2018) and his work has been published in *Asian Security*, *Defence Studies*, *Political Science* and with a variety of other leading academic publishers. Joe offers a variety of courses in Cyber Security, Strategic Studies and Security Studies and has extensive experience of professional and executive education in the military, defence and government sectors (e.g. NATO CCDCOE - Executive Cyber Seminar, New Zealand Defence Force Command and Staff College – NZDF CSC, Diplomatic Academy of Vietnam - DAV).

**Johanna Weaver** is Australia's expert to the United Nations' Group of Governmental Experts on responsible State behaviour in cyberspace, and Head of the Australian delegation to the United Nations' Open Ended Working Group on developments in the use of ICTs in the context of international security.

**Josh Gold** is a research assistant at the University of Toronto's Citizen Lab, and a Non-Resident Visiting Scholar at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). His research interests include global cyberspace governance, and military and intelligence cyber operations. Josh has closely followed and participated in the 2019-2020 UN Open-Ended Working Group discussions on international cybersecurity. Josh volunteers as a board member of both the Canadian International Council's Toronto Branch, and also of the Estonian Central Council in Canada. In 2019, he was a visiting fellow at the Hague Program for Cyber Norms, and an ICANN66 NextGen participant.

**Karuna Nundy** is an Advocate at the Supreme Court of India and an international lawyer who specializes in free speech, media and tech law; gender justice, constitutional and human rights law; and commercial dispute resolution. She serves on Columbia University's Global Free Speech Experts' Committee and the High Level Panel of Legal Experts for Media Freedom with Lord Neuberger and Amal Clooney. Ms. Nundy's work has been covered by the *New York Times*, the *Economic Times*, *Vogue*, *Forbes*, the *BBC*, among others. She has won some of India's most important cases on online free speech and other civil rights. Having studied at Delhi University in India, at Cambridge in the UK, and at Columbia in the US, her perspective is as local as it is international- she's qualified to practise in India and New York and has

advised the United Nations and many countries on law reform, as well as multinationals on cross border disputes.

**Ken Katayama** is a Policy Evangelist. He has been with Keio University Global Research Institute (KGRI) since 2018. He has been with Microsoft since 2007. Ken's role is to work with the government, academia and industry on cybersecurity policy issues to ensure a free, fair and secure cyberspace. He is also involved in issues related to the balance between privacy and data utilization. Ken is a member of several government committees such as "NISC-Committee to Promote a Safe Cyber Society", "METI- Cybersecurity Research Committee WG" , "National Police Agency-Cybersecurity Policy Committee", and "Tokyo Police Department- Public-Private Cybercrime Measures Committee". He is the Vice Chair of the Personal Data Protection Committee at JEITA and also has roles in other Japanese industry organizations such as the Keidanren and JCIC. He is an Executive Committee Member of the British Chamber of Commerce in Japan (BCCJ) for 2020-2021.

**Kerry-Ann Barrett** is the Cyber Security Policy Specialist at the Cyber Security Program at the Organization of American States. In her capacity she offers technical assistance to member states in the development and implementation of their national cybersecurity strategies as well as assist in the implementation of various technical capacity building initiatives within the Cyber Security Program. Additionally, in this capacity she has participated as a speaker at various regional and international cyberspace fora with a focus on cyber related issues in Latin America and the Caribbean. Kerry-Ann is also an attorney-at-law with over sixteen (16) years of experience. Included in her legal professional experience have been appointments within several government ministries in the Caribbean, as well as legal consultancy services to the CARICOM Secretariat and the ILO Sub-Regional Office for the Caribbean. She holds a Post Graduate Diploma in International Arbitration, a Master's in Business Administration (Distinction) in International Business, an LLB and Certificates in E-Diplomacy, Cyber Security Risk Management and Legal Frameworks for ICTs. Mrs. Barrett expertise covers cybersecurity policy development, electronic commerce, internet governance and cybersecurity. Most recently, she has led or provided technical support for the development of the national cyber security frameworks for countries such as Belize, Colombia, Costa Rica, Dominican Republic, Jamaica, México, Peru and Trinidad & Tobago. Her international experience includes the representation of the OAS in the Council of Europe, ICANN and has been designated 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 and the ICANN SSR2 Team.

**Laura Carpini** is the Head of Cyber Dept at the Ministry of Foreign Affairs in Rome. She joined the Italian Foreign Service in 1994, began her career at the Consulate General of Italy in New York from 1998 until 2002 and served in Cuba as Deputy Head of Mission at the Embassy of Italy until 2006, when she returned to Hqs in Rome. She was Human Rights Director until 2010, and led to success, in 2007, the first resolution on the moratorium of executions at the UNGA. In 2010 she was Head of the Political and Consular Sections in New

Delhi, served in Ghana as Ambassador 2012-2016, finally she was Diplomatic Advisor to the Mayor of Florence, from 2017 to 2019. Fluent in English, French and Spanish, she knows German and has notions of Portuguese. She received the honor of Officer Knight in the Order of Merit of the Italian Republic and she is a member of the Scientific Committee on “International Relations” of the Università per Stranieri in Perugia. Min. Plen. Laura Carpini is President the Association of female members of the Italian Foreign Service, DID. She is married and has a daughter.

**Laura Groenendaal** is Research and Projects Associate at the German Marshall Fund of the United States (GMF) in Brussels. She leads GMF’s EU-based cybersecurity work in cooperation with GMF’s Digital team and coordinates research and engagement activities of the EU-funded EU Cyber Direct project, particularly in relation to the EU’s bilateral engagement with Brazil and South Korea. In her research Laura focuses on EU cyber diplomacy and resilience including issues related to cyber security, cybercrime and data protection. Laura joined GMF in 2017 as a member of GMF’s Europe Program and worked on EU foreign policy. She obtained her master’s degree in European Public Affairs from Maastricht University in 2017 and has a bachelor’s degree in International Relations and International Organization from the University of Groningen.

**Louise Marie Hurel** is a PhD candidate in Data, Networks and Society at the London School of Economics and Political Science’s (LSE) Department of Media and Communications. Her research focuses on technical security expertise, cybersecurity governance, and incident response. She holds an MSc in Media and Communications (Data and Society) from the LSE, and a BA in International Relations from the Pontifical Catholic University of Rio de Janeiro (PUC-Rio). For more than five years, Louise Marie has continuously worked in the intersection between Internet governance and cybersecurity communities of practitioners. She leads research and cyber policy engagement at Igarapé Institute’s Cybersecurity and Digital Liberties Program, which includes, but is not restricted to projects related to the implementation of monitoring technologies for public security, IoT, and national cyber capacity building in Brazil. She also serves at the Advisory Board of the Global Forum of Cyber Expertise (GFCE) and the Advisory Group of Carnegie Endowment’s Partnership for Countering Influence Operations (PCIO). More generally, Louise Marie Hurel’s work focuses on exploring interdisciplinary approaches to contemporary security challenges, influence of big tech, the role of non-state actors in cyber norms, and regional and national Internet governance.

**Luca Belli**, PhD, is Professor of Internet Governance and Regulation at Fundação Getulio Vargas (FGV) Law School, where he heads the CyberBRICS project, and associated researcher at Centre de Droit Public Comparé of Paris 2 University. Luca is also Member of the Board of the Alliance for Affordable Internet (A4AI), Director of CPDP LatAm and member of the CPDP Programme committee. Before joining FGV, Luca worked as an agent for the Council of Europe Internet Governance Unit and served as a Network Neutrality Expert for the Council of Europe. Over the past decade, Luca has authored and edited more than 30 research outputs in English, French, Italian, Portuguese and Spanish, amongst which “De la gouvernance à la

régulation de l'Internet" (Berger-Levrault, 2016); the "Net Neutrality Compendium" (Springer, 2016); "Platform Regulations: How Platforms are Regulated and How They Regulate Us" (FGV, 2017) and "Gobernanza y Regulaciones de Internet en América Latina" (FGV, 2018) and the "Community Network Manual" (FGV-ITU-ISOC, 2018). Luca's works have been i.a. quoted by the Organization of American States Report on Freedom of Expression and the Internet (2013); used by the CoE to elaborate the Recommendation of the Committee of Ministers on Network Neutrality (2016); featured in the French Telecoms Regulator (ARCEP) Report on the State of the Internet (2018); used by the Brazilian Telecom Regulator (ANATEL) to define community networks (2020); and published or quoted by various media outlets, including The Economist, Le Monde, BBC, The Hill, China Today, O Globo, El Pais, and La Stampa.

**Madeline Carr** is the Director of the UK-wide Research Institute in Sociotechnical Cyber Security (RISCS) which looks at the human and organizational factors of cybersecurity. She is also the Director of the Digital Technologies Policy Lab which supports policy making to adapt to the pace of change in society's integration of digital technologies. Her research focuses on the implications of emerging technology for national and global security, international order and global governance. Professor Carr has published on cyber norms, multi-stakeholder Internet governance, the future of the insurance sector in the IoT, cybersecurity and international law, and the public/private partnership in national cyber security strategies. Her book *US Power and the Internet in International Relations* is published by Palgrave MacMillan. Professor Carr was the Co-lead on the Standards, Governance and Policy stream of the UK's £24M PETRAS research hub on the cyber security of the Internet of Things. She is now the lead on the Economics and Law lens of the new PETRAS National Centre of Excellence in Cybersecurity of the IoT. Professor Carr is a member of the World Economic Forum Global Council on the IoT. She is also the Deputy Director of a new Centre for Doctoral Training in Cybersecurity at UCL which focuses on the interdisciplinary nature of these problems.

**Mariya Gabriel** is the European Commissioner for Innovation, Research, Culture, Education and Youth since 2019. She also served as the Commissioner for Digital Economy and Society in the Juncker Commission (2017-2019). She is the first Vice-President of the EPP group and served as the Vice-President of the EPP Group in the European Parliament from 2014 to 2017.

**Mark Corcoral** is a PhD candidate at the Centre for International Studies (CERI) at Sciences Po Paris, in association with the Institute for Strategic Research (IRSEM). His research focuses on 5G security policy. His Master's dissertation on the US declaratory policy of publicly attributing cyber-attacks earned him the "Bastien Irondele Prize" awarded by the French Association on Warfare and Strategic Studies (AEGES), the "Junior Researcher Prize" awarded by the French Centre for Research in Intelligence (CF2R) and the "Scientific Prize" awarded by the Institute for Higher Studies in National Defence (IHEDN).

**Mihoko Matsubara** is Chief Cybersecurity Strategist, NTT Corporation, Tokyo, being responsible for cybersecurity thought leadership. She previously worked at the Japanese

Ministry of Defense before her MA at the Johns Hopkins School of Advanced International Studies in Washington DC on Fulbright. She served on Japanese government's cybersecurity R&D policy committee between 2014 and 2018. Mihoko is a prolific writer and has published articles from the Council on Foreign Relations, Lawfare, New America, the RUSI Journal, etc. She published a book on cybersecurity, attackers, defenders, and cyber threat intelligence in Japanese from the Shinchosha Publishing Co., Ltd in 2019. She has spoken at various engagements internationally such as RSA Conference 2018 and 2019 in San Francisco, the EU Cyber Forum 2019 in Brussels, and CyCon 2015 and 2019 in Tallinn, Estonia. She is Adjunct Fellow at the Pacific Forum, Honolulu, and Associate Fellow at the Henry Jackson Society, London.

**Michael N. Schmitt** is the Francis Lieber Distinguished Scholar at West Point's Lieber Institute. He is also Professor of Public International Law at the University of Reading (UK), Distinguished Scholar and Visiting Professor of Law at the University of Texas, and professor emeritus at the United States Naval War College. He was previously Chairman of the Naval War College's Stockton Center for International Law and Dean of the George C. Marshall European Center for Security Studies in Germany. Professor Schmitt served 20 years in the United States Air Force as a judge advocate specializing in operational and international law. In 1996 he graduated first in class from the Naval War College's College of Naval Warfare. From 2007 through 2008, Professor Schmitt occupied the Charles H. Stockton Visiting Chair of International Law at the Naval War College. He has been invited to serve as the Sir Ninian Stephen Visiting Scholar at Melbourne University, Visiting Distinguished Fellow at Emory Law School's International Humanitarian Law Clinic, Visiting Scholar at Australian National University and Visiting Scholar Yale Law School. Additionally, he has delivered the United Nation's Association (UK) Annual Ruth Steinkraus-Cohen International Law Lecture, James Crawford Lecture at Adelaide Law School, Sir Ninian Stephen Lecture at Melbourne University, Hilaire McCoubrey Lecture at Hull University and Waldemar Solf Lecture at the US Army's Judge Advocate General's Legal Center and School. The General Editor of the Lieber Studies series (OUP), Professor Schmitt serves on many boards of institutions, learned and professional societies, and publications dealing with international humanitarian law. A fellow of the Royal Society of the Arts and a member of the Council of Foreign Relations, in 2017 he was awarded the Order of the Cross of Terra Mariana by the President of Estonia for his contributions to cyber defence and in 2018 named the Naval War College's Research Scholar of the Year. Professor Schmitt has participated in multiple international expert working groups, including those on the Manual on the International Law of Air and Missile Warfare (Harvard Program on Conflict Research), Direct Participation by Civilians in Hostilities (ICRC), Characterization of Conflict (Chatham House), and, as Project Director, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. The author of over 160 publications, his works on law and military affairs have been published around the world. Professor Schmitt's academic degrees include a D.Litt (Durham University), JD (University of Texas), LL.M (Yale University), MA (Naval War College), and MA (Texas State University).

**Moonyati Yatid** is a Senior Analyst at ISIS Malaysia. Her expertise lies in areas related to technology and innovation, with a strong interest in digital society. This includes the nexus between the information disorder, society's well-being, new enabling technologies vis-a-vis digital privacy concerns. She has presented and published her research findings domestically and regionally. She holds a Ph.D. in Human-Computer Interaction from University of Sydney, Australia with her doctoral research work focusing on human's mental, physical and social behaviours and their interactions with collaborative software and hardware tools. She obtained her bachelor degree of Engineering in Design and Information Sciences, with a dissertation on integrating culture in designing groupware from Wakayama University, Japan.

**Moudhi Aljamea** has a PhD in Computer Security Algorithms Design from King's College London, Dr. Aljamea currently is the General Manger of the ICT School at STC Academy ( Saudi Telcom Company) as the first Saudi women who occupies an executive position in the company and she have a vast experience in cyber and information security. Prior joining STC, she was the president of entrepreneurship unit and business incubator and an assistant Professor in cyber security at Imam Abdurrahman Bin Faisal University, and considered as one of the Saudis experts in the computer security field. Her main field of interest is Cyber Security attacks in the Cyber war also, the use of (AI) Artificial Intelligence in Cyber security . She also takes an interest in the field of on-line digital identity in Social Media. Additionally, she develop many security algorithms, published several papers on them, and participated in many conferences around the world giving talks about her areas of expertise. Dr. Aljamea got one of the top professional certifications in computer Security (Certified Ethical Hacker V10) CEH which is an international well recognized certification in the cyber security field.

**Natalie Thompson** is a James C. Gaither Junior Fellow working with the Technology and International Affairs Program at the Carnegie Endowment for International Peace. Part of her current work at Carnegie focuses on the use of targeted financial sanctions for countering malicious cyber activity. Her research examines sanctions frameworks in the United States and European Union and compares sanctions with other nonmilitary instruments of statecraft aimed at deterring offensive cyber operations. In addition, she works on Carnegie's Partnership for Countering Influence Operations, a multi-sector effort to better understand and address the malign use of information to influence target audiences. Her broader interests relate to the impact of emerging technologies on state power and international security. Natalie holds a bachelor's degree in political science and mathematics from Kalamazoo College.

**Nayia Barmpaliou** is responsible for the cybersecurity public policy work of the World Economic Forum's Centre for Cybersecurity. She leads the Forum's initiatives that aim to address gaps in global public-private cooperation against cybercrime as well as on agenda setting efforts for public policy responses to systemic cybersecurity challenges. She is also managing the Centre's relationships with governments, international organisations, academia and civil society. Before joining the Forum, Nayia led the EU's dialogue and cooperation on cyber capacity building with governments and organizations internationally and spearheaded the effort in defining this policy area as a key tenet of the EU Cybersecurity Strategy. She was

also in charge of mainstreaming cybersecurity in the EU's development cooperation in parallel to designing and managing the EU's global and transregional multi-million external assistance programmes on cybersecurity and cybercrime. In her role she represented the EU in relevant international negotiations and fora at the UN and the Council of Europe, and advised on the impact of evolving cybersecurity policies and regulatory developments to international cooperation. She commenced her career as a barrister in Greece and worked for more than a decade in international relations and diplomacy focusing mainly on justice, security sector reform and human rights.

**Nibal Idlebi** is the chief of Innovation at UN-ESCWA. She is a senior policy expert in innovation and technology for development, information and knowledge society and digital and open government. She has extensively worked on identifying challenges and gaps and proposing policies for advancing knowledge society in the Arab region at national and regional levels. In her work she focused on enhancing enabling environment in the Arab region including cyber legislation, cyber safety, intellectual property systems, innovation and entrepreneurship and digital content. She has also wide expertise in digital transformation policy and institutional renovation based on digital technologies, openness and citizen participation. Ms. Idlebi leads as well regional projects and activities on innovation policy, digital content and entrepreneurship, emerging technologies for developing specific sectors and she is currently leading a project on open and innovative government. She is a member in several UN Working Groups such as the IATT-Work Stream 6, UN-e-Government Survey; and she represents ESCWA in a number of International and Arab working groups. She is also Jury Member of several Awards such as L'OREAL-UNESCO Award "For Women in Science", MIT Enterprise Forum Pan Arab Award and the World Summit Award (WSA). Dr. Idlebi has a computer engineering degree from "Ecole Supérieure d'Electricité" and a Ph.D on parallel and distributed systems from the Nancy 1 University in France.

**Paul Timmers** is research associate at the University of Oxford/Department of Politics and International Relations, where his current research focuses on cybersecurity in relation to sovereignty and strategic autonomy, as well as on AI and ethics. He is visiting professor at Rijeka University, Senior Advisor to the European Policy Center, Chief Adviser to the European Institute of Technology/Health, and Supervisory Board member of the eGovernance Academy in Estonia. He is CEO of iivii BV, which provides policy advice. Paul Timmers is a former Director at the European Commission for Digital Society, Trust & Cybersecurity. He was responsible for policy, legislation and innovation in cybersecurity, e-privacy, digital health and ageing, e-government / e-ID, and smart cities/mobility/energy. He was member of the Cabinet of European Commissioner Liikanen. For several years, he participated in the European Commission's Impact Assessment Board which scrutinizes policy and legislative proposals. Paul held various academic positions. He was manager in a large ICT company and co-founder of an ICT start-up, holds a PhD in physics from Nijmegen University in the Netherlands, an MBA from Warwick University in the UK, was awarded an EU fellowship at UNC Chapel Hill and completed executive cybersecurity education at Harvard.

**Patryk Pawlak** is the EUISS Brussels Executive Officer. In this capacity, he maintains and develops relations with other Brussels-based institutions. In addition, he is in charge of the cyber portfolio, leading the Institute's cyber-related projects and contributing to its outreach activities. Since June 2016, he is a member of the Advisory Board of the Global Forum on Cyber Expertise. His work on cyber-related issues and the European Union's security policies more broadly has appeared in several peer-reviewed journals and edited volumes. Patryk holds a PhD in Political Science from the European University Institute in Florence and an MA in European Studies from the College of Europe.

**Pavlina Pavlova** is an OSCE consultant with expertise in human rights, digital technologies and security policies. She is currently working on capacity building programmes for human rights defenders in Ukraine. As part of this activity, she co-ordinates delivery of the safety and security trainings for human rights defenders, including modules on digital security. Pavlina joined OSCE as the Liaison Officer of the Slovak OSCE Chairmanship to ODIHR with a task to foster relations between the Ministry of Foreign and European Affairs of the Slovak Republic and the OSCE institutions. She previously worked in the governmental institutions and international organizations based in Brussels and her home country - Slovakia covering a range of public policies and political issues. She is a graduate of KU Leuven with an MA (Hons) in European studies.

@PavlPavlova

**Patricia Esteve-González, Oxford Martin Fellow and GCSCC Research Fellow**

Since 2019, Patricia Esteve-Gonzalez is an Oxford Martin Fellow and a Research Fellow at the Global Cyber Security Capacity Centre (GCSCC), University of Oxford. Her work supports the multidisciplinary research programme of the project Cybersecurity Capacity Maturity Model for Nations. She has a PhD in Economics and her research interests are in Applied Microeconomic Theory, with a special focus on institutions, mechanism design, and competitions. Her published and ongoing research has applied empirical and theoretical methodologies in a variety of contexts - public procurement, affirmative action, European integration, and cybersecurity. Previously, Patricia worked at the Department of Economics of two different universities, University of Lancaster (UK) and Universitat Rovira i Virgili (Spain). She is an Associate Fellow of the Higher Education Academy and has experience in teaching a wide range of courses in Economics. She is currently teaching classes of the MPhil course in Microeconomics at the Department of Economics, University of Oxford.

**Philip Lark** is the Executive Director of the Program on Cyber Security Studies (PCSS) at the George C. Marshall European Center for Security Studies. Professor Lark is the Founder and Architect of the Marshall Center's Global Transnational Cyber Security Program. PCSS is a comprehensive non-technical strategic-level policy program specifically designed for top national leaders including diplomats, legislators, policy-makers, military and law enforcement officers, ministerial staffs, and cybersecurity professionals. He has over 30 years of international strategy, policy-making and planning experience in the cyber domain. His current

cybersecurity strategy, policy and capacity- building research and work is focused in Europe, Eurasia and Africa, focusing on designing and implementing whole-of-government solutions.

**Philippe Goffin** is the Minister of Foreign Affairs and of Defence of Belgium since 30 November 2019. Mr Goffin has been Mayor of Crisnée (Liège) since 2001 and was elected as a federal MP in 2010.

**Rachael Falk** is one of Australia's leading cyber security experts. As Chief Executive Officer of the Cyber Security Cooperative Research Centre, Rachael heads an innovative and dynamic program of collaboration between government, industry and universities. The Centre delivers world-leading cyber security research, creating commercial solutions to the ever-evolving problems of our interconnected world. And, led by Rachael, the Centre is helping ensure Australia's cyber security expertise, capability and resilience into the future. Rachael was Telstra's first General Manager of Cyber Influence and has a strong background in commercial law and cyber security, practising as a lawyer at top-tier firms and in-house for Telstra. She has also worked as a cyber security consultant and is co-author of the *Five Knows of Cyber Security*, setting an industry standard for organisational cyber security best-practice. Rachael holds an Advanced Masters in National Security Policy (Hons) from the National Security College (ANU), Bachelor of Laws (Hons) (UTS) and Bachelor of Arts (ANU).

**Ruhiya Seward** is a Senior Program Officer at Canada's International Development Research Centre, currently based in the Middle East Regional Office in Amman, Jordan. She supports a portfolio of research on digital governance, technology and innovation around the global South, and oversees IDRC's cyber policy think tank program. She has a Ph.D. in comparative politics (New School for Social Research), and an M.Sc. in International Relations (London School of Economics). Her most recent publication is *Making Open Development Inclusive: Lessons from IDRC Research* (MIT Press 2020) co-authored and edited with Matthew L. Smith.

**Simona Soare** is Senior Associate Analyst at EUISS working on United States defence policy, transatlantic security and defence, EU-NATO relations and defence innovation. Simona holds a PhD in Political Science/International Relations (2011) and has published extensively on transatlantic security and defence. Her latest publication focuses on transatlantic cooperation on defence innovation and emerging technologies and she is currently preparing a volume on *Rejuvenating Transatlantic Relations*, complete with important reflections on emerging technologies, data, space and their respective interplay for transatlantic defence. She is also editor of the upcoming Routledge volume on emerging technologies and international relations, scheduled for publication in the fall of 2020. Prior to joining EUISS, Simona served as advisor to the Vice-President of the European Parliament (2015-2019), working on transatlantic and European security, including the legislative files on European Defence Fund and political resolutions on defence-related research and development, military mobility and transatlantic relations.

**Sophia Ignatidou** is an Academy Associate at the International Security Programme of Chatham House, after completing the Stavros Niarchos Foundation Academy Fellowship there. She has been researching disinformation, artificial intelligence and tech policy, as well as data governance issues and continues to work as a freelance journalist. Sophia holds an MA in Journalism from Goldsmiths College and an MA/PGDip in International Studies and Diplomacy from the School of Oriental and African Studies, London.

**Tatiana Jančárková** is a researcher at the Law Branch of NATO CCDCOE. Her current research interests include application of international law to cyberspace operations (Interactive Cyber Law Toolkit project), protection of critical information infrastructure and cybersecurity related aspects of 5G technologies. She has previously served as legal adviser and the Head of International Organisations and Law unit at the National Cyber and Information Security Agency of the Czech Republic and has practised in the fields of human rights law and international criminal law. Ms Jančárková holds master's degrees in law and in Russian and East European studies from Charles University in Prague and an LL.M. in public international law from Leiden University.

**Teki Akuetteh Falconer** was the first Executive Director to set up the Data Protection Commission of Ghana and facilitated the implementation of Ghana's Data Protection Act until her exit in July 2017. She is a Senior Partner at Nsiah Akuetteh & Co. a law firm based in Accra, Ghana that specializes in information technology and telecommunication law in Africa. She is a privacy and data protection consultant and has previously worked for the Government of Ghana in the development of several key legislation for the ICT sector including the Data Protection Act, 2012 (Act 843), Electronic Communications Act, 2008 (Act 775) and Electronic Transactions Act, 2012 (Act 772). She has also worked in various capacities with regional bodies such as ECOWAS. She is a member of the UN Global Pulse Privacy Advisory Group and a member of advisory committee for the 40th International Conference of Data Protection and Privacy Commissioners. She holds an LL.M. in Information Technology and Telecommunications Law from the University of Strathclyde, Glasgow – Scotland and a Bachelor of Arts in Law and Political Science from the University of Ghana (Legon), Accra – Ghana.

**Tjerk Timan** (MA, Ph.D., Male) currently works as a policy analyst at TNO, The Netherlands. In this position he works on projects such as the BDVA, the Once – Only Principle, and projects related to Privacy-by-Design in the age of (big) data, and fairness and transparency in AI. Common questions in these projects evolve around societal and organizational embedding of novel ICTs and the potential impact of new technologies on different actors. He brings both academic-and professional experience to the field, having worked as a Postdoc researcher on the project 'Privacyspaces – redefining privacy for the 21st century' at the Tilburg Institute for Law, Technology and Society (TILT); on ICT and user studies at the university of Twente at the Science, Technology Policy (STePS) department; teaching big data and visualization methods at the Erasmus University of Rotterdam and for NGOs and the wider public; and he

has been developing and testing software and online environments for several commercial parties ( Philips Eindhoven, freelancer for several SME clients). He was one of the first to research the impact of bodycameras in the Netherlands and he has worked in the field of law enforcement technologies. Tjerk was a visiting scholar at the Management school of St. Andrews University, Scotland and has published and presented about data, devices and values-by- design matters in f.i. Philosophy of Technology, Engineering Ethics, OUP, Environment and Planning A, Surveillance & Society and he has published books on Privacy in Public Spaces. He is currently investigating the relation between data, AI and the way in which data-driven developments impact daily (data) practices.

**Tinatin Akhvlediani** is a Researcher at CEPS' Foreign Policy unit. Her expertise and publications are focused on ICT and trade. Her geographic area of expertise is Eastern Partnership with a specific focus on the EU's Association Agreements with Georgia, Moldova and Ukraine. Before joining CEPS, she worked as a research assistant at the Digital Economy Lab, jointly established by the University of Warsaw and Google, and as an academic assistant at the College of Europe. Since 2017, Tinatin has been leading a research project granted by the National Science Centre of Poland on ICT and trade in Central and Eastern Europe. On this topic, she conducted research visits at Indiana University in the United States, Vienna Institute of International Economic Studies in Austria and Shanghai University in China. Her research outcomes have been presented at the international conferences in Europe as well as in Canada, United States, China, Australia and Thailand. Tinatin holds a PhD degree in Economics from the University of Warsaw, Master's degrees in International Economics from the University of Warsaw and European Economic Studies from the College of Europe and a Bachelor's degree in Economics from Tbilisi State University.

**Wiktor Staniecki** is the Head of Cyber Sector in the Security and Defence Policy Division at the European External Action Service. Before assuming this position, he was posted to Tokyo, working in the Political Section of the EU Delegation to Japan. Within the European External Action Service, Mr Staniecki also worked as desk officer for Brazil (2013-2015) and the United States (2008-2013). Previous to his work for the EEAS, he was a consultant at Burson-Marsteller Brussels and worked for the European Commission on entrepreneurship policy. Mr Staniecki holds Master's Degree of European Studies from Adam Mickiewicz University in Poznan, Poland, as well as Diplôme d'Etudes Générales Européennes of Centre Européen Universitaire de Nancy 2.

**Xymena Kurowska** is an International Relations theorist interested in interpretive policy analysis. She received her doctorate in political and social sciences from European University Institute in Florence, Italy. She works within international political sociology, with a particular focus on security theory, psychosocial and anthropological approaches in the study of politics, relational and interpretive methodologies, and the ethics of academic practice. She has been a grantee of European Foreign and Security Policy Studies Programme and a Marie Skłodowska-Curie senior research fellow at the Department of International Politics at Aberystwyth University. She also served as the CEU principal investigator in Global Norm Evolution and

Responsibility to Protect, chair of International Political Sociology section at International Studies Association, and academic rapporteur for EU Cyber Direct. She co-edits Palgrave book series Central and Eastern European Perspectives on International Relations and serves on the editorial board of PARISS: Political Anthropological Research on International Social Sciences.

**Yuliya Miadvetskaya** is a researcher at the Centre for IT & IP Law at KU Leuven University. She works on Infrastress (cybersecurity) and TRUSTS (data markets) research projects. Prior to this, she worked as an academic assistant at the Department of European Legal Studies at the College of Europe and interned with the Legal Service of the European Parliament in Brussels. She holds an LLM in European Law from the College of Europe. Her research interests lay primarily in the area of cybersecurity, sanctions, EU external relations and data protection.