Workshop

The Dilemmas of Attribution: Between Politics and Law

Leiden University, Institute of Security and Global Affairs and

EU Cyber Direct project

24 May 2019, Peace Palace, The Hague

THE HAGUE PROGRAM for Cyber Norms

Universiteit Leiden

EU CYBER DIRECT

Overall goal of the workshop

While the general idea that attribution is a political process is not controversial in itself, the criteria for arriving at the decision to attribute are highly contested. The main disagreement is linked to the question about certainty and what evidentiary standards need to be met for a decision about attribution to be legitimate and lawful. One camp in this debate is focused primarily on the decision to attribute as a means to deter malicious actors. Due to the political nature of such decisions, the main risks associated with these decisions are political and reputational. This contrasts with another approach grounded in the rule of law and due process which sees the decision about attribution not as the final objective but as one step in imposing the consequences on malicious actors. The risks in such cases are not only political but have significant bearing on legitimacy and legality of the concrete measures adopted as a result of the legal and procedural standards that the evidence has to meet. Both processes require evidence, but the standards are very different. Proponents of political attribution fear the lawlessness of a space in which unacceptable behaviour has no consequences; proponents of the more legalistic approach fear the lawlessness of a space in which consequences are the result of politics and not of international (criminal) law. Consequently, the aim of this workshop is to reflect on the dilemmas linked to the question of attribution in cyberspace:

- What *evidentiary standards* are dictated by the international law and criminal proceedings and under what circumstances?
- Is there a *threshold* that needs to be met for attribution to specific states and how does that correspond to criminal law and international law? To what extent does indicting individuals also mean indicting a state?
- How can evidence from intelligence agencies play a role? What other sources of evidence play a role in this process?
- How to publically communicate the decisions about the attribution and what are the roles of different stakeholders in this process?

The workshop is divided into a plenary opening and a plenary closing session and two breakout sessions in between. Each session will have one or more short introductions to set the scene and get the debate going. Throughout the day, our aim is to tease out differences and commonalities in the respective approaches (international law, criminal law, policy perspective) to the main stages of the attribution process: suspicion, accusation, and consequences. For that reason we have invited participants from different backgrounds who can help us look at the attribution process through their respective disciplinary lenses. We are interested in particular in your thoughts about the legality of actions taken by a state-victim or its allies and the evidentiary standards for such decisions.

Workshop Schedule

23 May 2019		
18:30 – 21:00	Dinner	Restaurant Oker

24 May 2019		
08:45 – 09:30	Arrival / Coffee & tea	Peace Palace
09:30 – 09:45	Welcome / Introduction	Historische Leeszaal
09:45 – 11:15	**Plenary Session – Why do we attribute? Linking policy objectives and the process**	**Historische Leeszaal**
11:15 – 11:30	Short break	
11:30 – 13:00	**Breakout Session I – From suspicion to accusation**	**A: Historische Leeszaal** **B: Bestuurskamer**
13:00 – 14:00	Lunch break	
14:00 – 15:30	**Breakout Session II – From accusation to consequences**	**A: Historische Leeszaal** **B: Bestuurskamer**
15:30 – 16:00	Coffee break	
16:00 – 17:30	**Plenary Session – What next for the attribution debate: Legal, policy and political dilemmas**	**Historische Leeszaal**

CONTACT INFORMATION

Dennis Broeders   +31 (0)6 180 707 69
Corianne Oosterbaan +31 (0)6 106 205 31
Patryk Pawlak   +32 (0)488 813 980

SESSIONS

Plenary Session I (09:45 – 11:15): Why do we attribute? Linking policy objectives and the process

Chair: *Patryk Pawlak*
Speakers: *Nicholas Tsagourias (International law perspective)*
                Tatiana Tropina (Criminal law perspective)
                Florian Egloff (Policy/politics perspective)

Attribution of a cyber operation is not – or should not – be an aim in itself. It is strictly linked to a broader objective that a state or a group of states wishes to achieve, i.e. signalling, deterrence, naming and shaming, etc. Depending on the overall policy goal, the process of attribution embodies several concrete choices and dilemmas. The purpose of this session is to link the process of attribution with concrete actions and policy choices that governments have – ranging from issuing a statement to criminal prosecution or imposition of restrictive measures – in order to identify legal and operational questions associated with this process (i.e. what is evidence, what prescribed legality of an action, etc.). By now, we have quite some case material about attributions taking both the legal route (DoJ cases) and the more political route, either unilateral or in the form of attribution coalitions (see also the attached background note). One of the main questions to be answered at this stage is: where do we draw the line between what is political and legally acceptable? Consequently, this session will also look at the motivations of the states not to attribute certain attacks as part of the broader foreign policy approach.

Breakout Session I (11:30 – 13:00): From suspicion to accusation

Breakout group I A: Patryk Pawlak (Chair), Mary Ellen O'Connell (Input giver)
Breakout group I B: Els De Busser (Chair), Arun Sukumar (Input giver)

This session will focus on the initial stages of the response formulation, which might eventually result in attribution of a cyber operation. The aim of the session is to answer how states substantiate their suspicions about a wrongdoing by another actor and what evidentiary requirements need to be met to actually (publically) accuse another state (and/or individual state operatives). Suspicion has to be internally substantiated by investigation, collecting and assessing the evidence, and the formulation of policy options. The step towards public accusation repeats some of those steps but has to take into account the international context and expect scrutiny of any decision to accuse by other states. Accusation requires analysis and assessment of the evidence, degree of certainty as a factor, and criteria for a decision to accuse (accuse a state or a group, why is a state responding).

- The focus is on the threshold value(s) that allows evidence to be translated into an accusation: both public and in bilateral relations between the countries concerned. What are the rights and obligations of states in such cases (e.g. the right to respond but also the obligation to assist in solving the problem or take into account all circumstances)?
- What are (minimum) evidentiary standards? What is the burden of proof?
- What is the relation between trust and the reliability of sources and information (relevant in light of the fact that sources are often intelligence sources)?
- What is the role of attribution coalitions (also in terms of evidence sharing and trust)?

Breakout Session II (14:00 – 15:30): From accusation to consequences

Breakout group II A: Patryk Pawlak (Chair), Marco Roscini (Input giver)
Breakout group II B: Dennis Broeders (Chair), Dan Efrony (Input giver)

This session will discuss the next stages in the response formulation, in particular the move from accusation to imposing consequences, which also requires a separate political decision that is directly linked to attribution. Public attribution can be seen as the end game of the process, or as a necessary step towards the decision to implement consequences. The debate about consequences is also a debate about evidentiary standards, but has only scarcely begun. Consequences require thinking about concrete actions that states can take, the elements that drive particular decisions, the evidentiary standards attached to these choices, and the question of the legality and legitimacy of (counter) measures under international law.

- The focus is on the threshold value(s) that allows a (public) accusation to be translated into the imposition of consequences on the accused.
- What are threshold values for imposing consequences (assuming we are *under* the threshold for armed conflict)? What are the triggers under international law, criminal law and in policy?
- How formal should consequences be formulated in advance (EU sanctions regime versus American strategic ambiguity)? What are pros and cons of each approach? (bearing in mind that 'non consequences' is still pretty much the prevailing norm).
- How do you determine the legality/legitimacy/proportionality of consequences (both the original act and the reaction can be expected to be legally and politically scrutinized)?

Plenary Session (16:00 – 17:30): What next for the attribution debate – legal, policy and political dilemmas

Chair: Dennis Broeders

The purpose of this session is to summarise and compare notes from the discussions in the breakout sessions. The aim is to identify the gaps in our understanding of the legal, policy and political dilemmas linked to the topic of attribution. What are open questions that we have not addressed and merit more attention? What are larger issues that require more scholarly attention? And lastly, recognizing that these decisions belong ultimately to states, are there any concrete recommendations that we can propose or any initiative that we are aware of that respond to some of these challenges?

LIST OF PARTICIPANTS

Name	Organisation	Group
Daniel Alvarez	University of Chile, Faculty of Law, Chile	A
Benjamin Ang	S. Rajaratnam School of International Studies, Singapore	B
Lorena Bachmaier Winter	Universidad Complutense Madrid, Spain	B
Dennis Broeders	The Hague Program for Cyber Norms / Institute of Security and Global Affairs, Leiden University, The Netherlands	B
Els De Busser	The Hague Program for Cyber Norms / Institute of Security and Global Affairs, Leiden University, The Netherlands	B
Dan Efrony	Hebrew University of Jerusalem, Israel	B
Florian Egloff	ETH Zürich, Switzerland	A
Monica Kaminska	Oxford University, United Kingdom	B
Kubo Mačák	University of Exeter, United Kingdom	A
Mary Ellen O'Connell	University of Notre Dame, United States	A
Patryk Pawlak	EU Cyber Direct / European Union Institute for Security Studies (EUISS)	A
Marco Roscini	University of Westminster, United Kingdom	A
Arun Mohan Sukumar	Observer Research Foundation (ORF), India	B
Stanislaw Tosza	Utrecht University, The Netherlands	B
Tatiana Tropina	Max Planck Institute for Foreign and International Criminal Law, Germany	A
Nicholas Tsagourias	University of Sheffield, United Kingdom	B
Frank Verbruggen	Leuven University, Belgium	A
Mario Viola	Institute for Technology & Society (ITS) Rio, Brazil	A