Attribution of Cyber Attacks – Workshop Summary

On June 6th, 2019, a workshop on *Attribution of Cyber Attacks* took place in Rotterdam. The workshop was part of a research program on *attribution of cyber attacks*, led by Professor Yuval Shany (*The Federmann Cyber Law Program Director at Hebrew University*), Professor Michael N Schmitt (*Chair of Public International Law at Exeter University and general editor of the Tallinn Manuals*) and Professor Paul Ducheine (*University of Amsterdam and Netherlands Defense Academy*) and supported by the Federmann Cyber Security Center in collaboration with the Dutch Ministry of Foreign Affairs

This multidisciplinary workshop brought together experts from diverse scientific, legal, and public-policy fields, as well as from various institutions including academic institutions, NATO, National police, Google, private consultancies. Six members of the Federmann Cyber Security Center participated and presented preliminary findings: Professor Yaël Ronen, Major-General (ret.) Dan Efrony, Dr. Thibault Moulin, Mr. Nimrod Karin, Mr. Jack Kenny and Mr. Michael Cohen-Ad. Additional international participants were: Ashley Deeks (*University of Virginia School of Law*), Jon Ford (*FireEye Mandiant*), Liis Vihul (*Cyber Law International*), Duncan B. Hollis (*Temple University School of Law*), John Davis (*Google*), Gert Ras (*Team High Tech Crime at NLD Police*), Isabella Brunner (*Bundeswehr University Munich*), Karine Bannelier (*Grenoble Alpes University*), Marjolein Busstra (*Dutch Ministry of Foreign Affairs*), Ronald Prins (*Member of the TIB, the Kiesraad and Associate member of the Dutch Safety Board*), Steven Hill (*The Office of Legal Affairs at NATO*), Terry Gill (*University of Amsterdam*) and Theodore Christakis (*Grenoble Alpes University*).

This workshop was the second in a series of three. The first one was held in Jerusalem in November 2018. While the first workshop was dedicated mostly to the technical aspects of the attribution, the current workshop was dedicated to the attribution's legal dimensions and to comparative attribution models.

The workshop sought to explore the viability of an international attribution mechanism; its possible structure, authority, process, and scope of authority; and the role that such a mechanism could play in light of the legal framework governing cyber operations.

The first session of the workshop addressed legal dimensions of attributing the conduct of private actors to states. The indeterminacy regarding the standard of conduct by a state that would render it responsible under international law standards for the conduct of a non-state actor, and the level of proof required for attribution to be legally valid to a state, were underscored. With regard to the former it was noted that there is preliminary issue of characterizing specific cyber operations as violations of international law, particularly their characterization as 'armed attack' and as violation of state sovereignty. Note was taken of novel questions that have arisen with regard to links between non-state actors and their host states which may render the latter responsible for conduct of the former, such as in cases of hack-back. Participants discussed the link between the level of proof required for attribution and the purpose for which attribution would be sought, distinguishing between attribution for the purpose of attaching legal responsibility by an international legal or quasi-legal mechanism, and attribution for the purpose of unilateral measures by a victim state in response to a cyber-attack, under doctrines such as self-defense, countermeasures and retorsion. It was also proposed that the standard of proof may differ depending on the seriousness of the conduct at issue. Practical difficulties were considered, such as states' reluctance to share evidence and their need to respond quickly, while attribution procedures remain relatively slow.

A second session concerned lessons learned from past attribution attempts. Participants provided an overview and analysis of case studies of cyber operations where states and private companies have attempted to attribute those operations to specific actors and in some instances to states who are affiliated with those actors. A number of instances where states attributed cyber operations to other states were considered. Such attribution case studies took various forms, including general statements of attribution of a legal character, attribution on the political level, as well as through domestic indictment of individuals. The cooperation between the private sector attribution agencies and government agencies was highlighted, particularly with regard to technical details. It was suggested that best practices include the adoption of precise threshold of confidence that would legitimately substantiate attribution as well as reliance on technical data, and distinction among cyber operations according to their severity. Particular attention was given to the value of collective attribution, as a factor which increases the credibility of the attribution and is likely to generate greater legitimacy with regard to the choice of response.

It was suggested that existing practice disproves some working assumptions. For example, contrary to expectation, states do not make attribution statements, including on the political level, unless they have a high level of confidence in the outcome. It was noted that only general statements of attribution were made, with sparse technical analysis or support for the findings. Also, while evidence-sharing is an issue that needs to be tackled, it is not always an obstacle as there is a lot of openly available information. On the other hand, the object of attribution often remains vague, given the controversy over the characterization of many cyber-operations as violations of international law. Since substantive law on the matter develops through the practice of states, attribution also changes over time.

The third session concerned existing and prospective international mechanisms of attribution in other subject-matter contexts. Those deal primarily with nuclear weapons verification regimes. It was highlighted that their role was primarily technical, and they support the importance of creating multi-stake holder coalitions. Participants overviewed existing attribution mechanisms such as the IAEA which includes fact-finding reports and on-site inspections, the OPCW which includes verification and confidential attribution reports, the CTBTO which provides a 24/7 tracking of nuclear tests and features an attribution mechanism, and the PSI which comprised of enforcement cooperation.

Moreover, proposed attribution mechanisms such as those of the Multilateral Cyber Attribution and Adjudication Council (MCAAC), the International Cyberattack Attribution Organization and the Global Cyber Attribution Consortium (GCAC) were reviewed. Participants discussed the significance of attribution as a 'naming and shaming' process. It was highlighted that although this is not a legal process, it has an impact on the development of international norms, and is dependent on their existence. Attribution can also induce compliance. The impact of specific attributions depends on a variety of factors, such as the level of information exposure, the relationship between the accuser and the accused, and the strength of the condemnation. Again the advantages of collective accusation were highlighted, especially in relation to creating law through custom.

The value of an independent, global organization whose mission consists of investigating and publicly attributing major cyber-attacks was also discussed. This organization, participants suggested, will produce standardized and transparent attribution that may overcome concerns about credibility. Looking ahead towards a prospective international cyber attribution organisation, participants discussed issues that would require consideration. These include the level of reliance on private sector actors, transparency of operation modalities and evidence assessment. It was queried whether and how politicisation can be avoided. In this and other contexts the significance of determining who would be entitled to initiate a process was noted.

In the final session, participants highlighted core issues that arose from the workshop as requiring and meriting further investigation. With regard to the legal aspects, these include the role of collective attribution; the type of conduct that should be within the scope of the mechanism; the question whether attribution should be restricted to states or expanded also to private actors; and the evidentiary standard that should be applied. As for institutional issues, those include the role of the private actors within the mechanism; measures to ensure the effectiveness and legitimacy of the mechanism, including selection criteria; and forms of cooperation between law enforcement agencies, intelligence bodies and sharing and collective initiatives.

Among the pending questions, one may note the following:

- How should one deal with the notion that attribution is a political prerogative and not a legal institution?
- What functions can a new attribution mechanism, focusing on the responsibility of states, play in international life and what are the geopolitical conditions that would render it viable/unviable?
- should the mechanism be purely focused on state responsibility, or rather also cover the responsibility of private actors?
- How should an inter-state mechanism relate to private mechanisms and to the work of government and private security agencies and to civil society initiatives such as citizen lab?
- What guarantees need to be put in place to ensure the independence, impartiality, effectiveness and legitimacy of any new mechanism?
- How could such a mechanism facilitate cooperation between law enforcement agencies, intelligence sharing and collective attribution initiatives.
- How should such a mechanism deal with the thorny problem of espionage?
- What contribution can such a mechanism have in the area of data collection, and harmonisation of approaches and terminologies in the field?

- Should a mechanism deal with specific security challenges only (e.g., terrorism? Election manipulation)? Or with a specific form of cyber risk (e.g., attacks on BGP, global attacks)? Or with merely linking the attack to a certain computer/territory?
- What case selection principles/thresholds should govern the work of the mechanism? What evidentiary standards it should follow?
- Should the mechanism engage in prevention - through using predictive algorithms, warning sensors, detection of patterns? Should it engage in dissemination of information on best practices and capacity development?
- Does the Budapest Convention has any role to play in the new mechanism? Does the EU tool box?
- Who is likely to use the mechanism (inter alia in light of the existing patterns of inter-state accusations)

Future plans

In the following months the research team will work on 3-4 papers that will be published in academic journals.

Furthermore, the third workshop on the political viability of an international attribution mechanism will be held in Chatham House London in January 2020.

Appendix I: The Workshop's Agenda

June 5th – 21:00-23:00

Cocktail Meeting at the Inntel Hotel Rotterdam – Waterfront Restaurant

June 6th

09:00 – Gathering and Introduction

09:15-10:30 – Panel I: The Attribution Problem: Legal Dimensions

Ashley Deeks, University of Virginia School of Law – *Legal Dimensions of the Cyber Attribution Problem*

Discussant: **Yael Ronen**, The Hebrew University of Jerusalem

10:30-10:45 – Coffee Break

10:45-12:00 – Panel II: Lessons Learned From Past Attribution Attempts

Jack Kenny, The Hebrew University of Jerusalem – *The Prospects for an International Attribution Mechanism for Cyber Operations: Lessons Learned from Past Attribution Attempts*

Jon Ford, FireEye Mandiant – *HUman Network Targeting (HUNT): Lessons in Attribution*

Liis Vihul, Cyber Law International – *How Are Public Attributions of Cyber Operations Shaping the Normative Regime of Cyberspace?*

12:00 – Lunch

13:30-14:45 – Panel III: Comparative Attribution Models

Dan Efrony, The Hebrew University of Jerusalem – *An International Attribution Mechanism – Is It Required? Is It Practical?*

Duncan B. Hollis, Temple University School of Law – *Beyond Naming and Shaming: Accusations and International Law in Global Cybersecurity*

John Davis, Google – *Options for an International Cyber Attribution Organization*

14:45-15:15 – Coffee Break

15:15-17:00 – Panel IV: The Road Forward – Concluding Remarks

Michael Schmitt, University of Exeter

Paul Ducheine, University of Amsterdam

Yuval Shany, The Hebrew University of Jerusalem

18:00 – Dinner at the Euromast Restaurant (Parkhaven 20, 3016 GM Rotterdam)

Discussants (alphabetically)

Gert Ras, Team High Tech Crime (NLD Police)

Isabella Brunner, Bundeswehr University Munich

Karine Bannelier, Grenoble Alpes University

Marjolein Busstra, Dutch Ministry of Foreign Affairs

Michael Cohen-Ad, The Hebrew University of Jerusalem

Nimrod Karin, The Hebrew University of Jerusalem

Ronald Prins, Member of the TIB, the Kiesraad and Associate member of the Dutch Safety Board.

Steven Hill, Legal Adviser and Director of the Office of Legal Affairs at NATO

Terry Gill, University of Amsterdam

Theodore Christakis, Grenoble Alpes University

Thibault Moulin, The Hebrew University of Jerusalem