ICT for peace foundation

Meeting Report: Workshop on Trusted Attribution in Cyberspace

Summary

On 29 and 30 August 2019, ICT4Peace Foundation, with support and sponsorship from the German Federal Foreign Office, conducted a two-day workshop on trusted attribution in cyberspace. The workshop was organised with the intention of inciting debates among key stakeholders concerning different attribution practices and the idea of creating an independent network of organisations engaging in peer-review assessments and substantive analyses. The workshop was attended by more than twenty representatives from civil society, industry, academia, and governments and conducted under the Chatham House rule.

Among other things, participants engaged in discussions around key stumbling blocks related to trusted attribution practices in cyberspace and potential mitigating activities. They also devised a number of criteria/strategies for effective collaboration setups and reported on related processes pursued in other fora.

Participants agreed that there is value in raising the consequences for perpetrators in cyberspace through shared, network-based attribution practices. It was noted, however, that rather than focusing on blame ascriptions and finger-pointing exercises, there is greater merit in carrying out peer-centred fact-finding and review activities. It is planned to take the discussions held on 29 and 30 August 2019 forward and launch peer-review and information-sharing exercises around a test case.

Author: Jacqueline Eggenschwiler

Introduction

This report offers a synopsis of the main insights gathered during the two-day workshop on trusted attribution in cyberspace, organised by ICT4Peace Foundation in collaboration with the German Federal Foreign Office, and summarises the preliminary results agreed upon. Participant comments and inputs delivered over the course of the workshop are presented in anonymised form. Apropos structure, the report follows the chronology of the workshop, and first recapitulates the main points gathered on day one, before summing up the key messages communicated on day two.

Day One, 29 August 2019

The first day of the workshop began with welcoming remarks by Felix Haala, German Federal Foreign Office, and Daniel Stauffacher, ICT4Peace Foundation. After the opening statements, the session conveners provided background information on the structure and goals of the workshop.

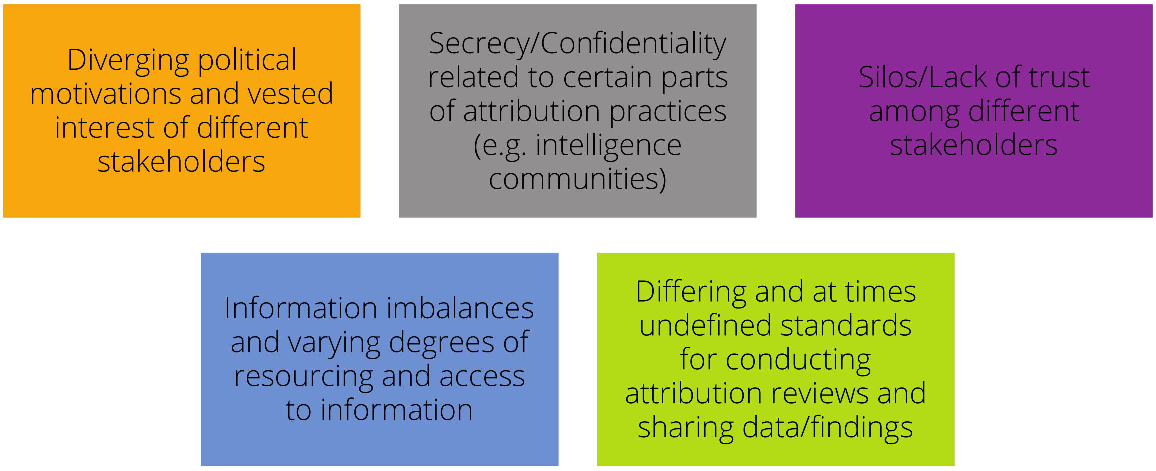
The workshop was pursued with the following objectives in mind:

- Gather and foster exchanges among different stakeholders concerning trusted attribution in cyberspace
- Put forward recommendations for addressing identified gaps in current attribution practices and share best-in-class cases
- Discuss and map out the contours of an independent network of organisations engaging in attribution peer-review
- Contribute to achieving an open, secure, stable, accessible, and peaceful cyberspace, and reduce the risks to international peace and security

The workshop convenors reiterated that as the numbers and effects of malicious activities conducted in and through the virtual realm continue to proliferate and worsen respectively, it is critical to devise collaborative solutions and work on measures to increase the consequences for perpetrators, and strengthen the resilience and stability of digital domain.

Subsequent to the presentation of the workshop goals, participants were asked to conduct a brainstorming exercise around the key stumbling blocks constraining trusted attribution practices in cyberspace, and measures to mitigate them. To allow for variation and diversity in terms of answers and outcomes, participants were split into four breakout-groups.

Based on the responses of the four groups, five key areas hampering effective attribution practices were identified, namely:



Diverging political motivations and vested interest of different stakeholders

Secrecy/Confidentiality related to certain parts of attribution practices (e.g. intelligence communities)

Silos/Lack of trust among different stakeholders

Information imbalances and varying degrees of resourcing and access to information

Differing and at times undefined standards for conducting attribution reviews and sharing data/findings

Figure 1: Key factors hampering effective attribution practices

With regard to mitigation measures, participants suggested that rather than trying to unknot political divergences and differing ideological standpoints, attribution processes should take into account and be structured around theses inhibitors.

They maintained that trust relationships and confidence-based interactions among different stakeholders are key building blocks for successful attribution practices and shared event histories. At the same time, however, participants reasoned that attribution practices may benefit from temporary exclusion principles relating to certain stakeholders during certain stages of attribution investigations. For instance, they argued that with a view to minimising political controversies, governments should not be involved in all stages of attribution investigations.

Participants further contended that attribution processes should not only focus on high-profile or large-scale cyberattacks but also address lower-level incidents, which have the potential to inflict harm. Moreover, attribution processes should harness the plurality of methods put forward by different stakeholders and be organised around effective data sharing and collaboration arrangements.

Subsequent to the discussions on key stumbling blocks, a number of participants reported on attribution efforts conducted across other fora. For instance, representatives from the Citizen Lab at University of Toronto, the Internet Governance Project at Georgia Institute of Technology, and the Center for Security Studies (CSS) at Eidgenössische Technische Hochschule (ETH) Zürich shed light on the complementary (or possibly even overlapping) activities of the Transnational Attribution Working Group, a multi-stakeholder oriented collection of university-based organisations and independent researchers, which seeks to facilitate transnational, independent, and neutral attribution processes.

The first day of the workshop concluded with discussions around ICT4Peace Foundation's proposal for the creation of an independent network of civil society organisations, industry representatives, and governments, subscribing to shared attribution principles and protocols and engaging in attribution peer-reviews.

Day Two, 30 August 2019

The second day of the workshop was structured around a mind-mapping exercise. Following a brief recapitulation of the debates held on day one, participants were asked to sketch out key features of a network of organisations committing to execute attribution peer-reviews.

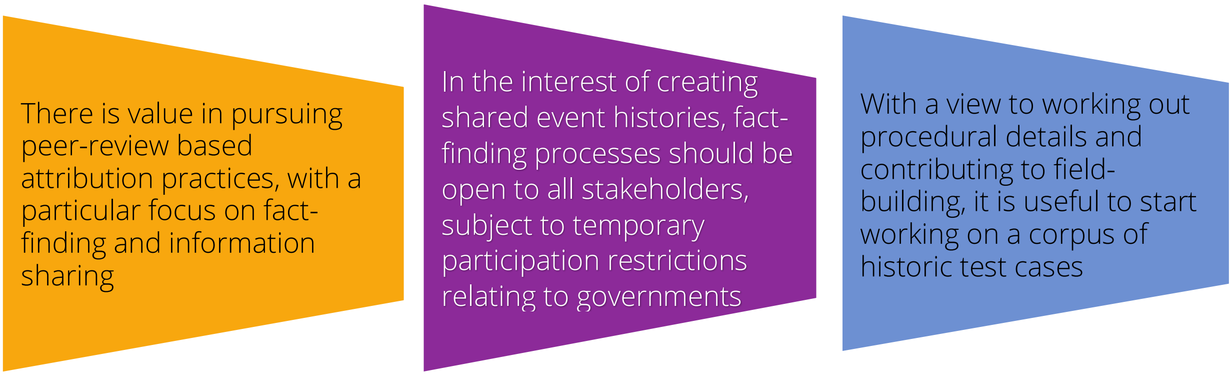
While a great many questions concerning, for instance, membership structure, selection criteria, investigation methodologies, and collaboration agreements were touched upon, organisational and procedural aspects in connection with the establishment of a network of organisations engaging in attribution peer-reviews remained fairly elusive.

Despite modest levels of structural clarity, however, participants agreed that building a network of entities conducting attribution peer-reviews, with the intention of raising the stakes for perpetrators and ensuring peace and stability in the virtual realm, holds value and is worthwhile being pursued further. They noted however, that rather than focusing on (public) blame ascriptions and finger-pointing exercises – exercises which are (potentially) politically sensitive – there is greater merit in carrying out peer-centred fact-finding and review activities (at least ad interim).

Participants were also cautious enough to reiterate that while in the interest of creating shared event histories it is important to have different stakeholders represented, further clarifications are necessary as to when (at which stages) and how (in which capacities) different stakeholders, especially governments, should participate in and contribute to the proposed fact-finding processes.

With the intention of resolving some of the open questions surrounding the creation of a network of organisations sharing and assessing attribution-relevant data and information, participants proposed the execution of a test case. Structuring interactions and analyses around a test case could help spec out procedural details and mitigate obstacles to data and information sharing early on, participants

In a nutshell, participants concurred that:



There is value in pursuing peer-review based attribution practices, with a particular focus on fact-finding and information sharing

In the interest of creating shared event histories, fact-finding processes should be open to all stakeholders, subject to temporary participation restrictions relating to governments

With a view to working out procedural details and contributing to field-building, it is useful to start working on a corpus of historic test cases

Figure 2: Workshop outcomes

Way Forward and Next Steps

Inspired and motivated by the high levels of engagement exhibited by the participants over the course of the workshop, ICT4Peace Foundation plans to take discussions forward and explore the possibilities for conducting fact-finding exercises around a test case. It strives to conduct another workshop in summer 2020 (tentative).

ICT4Peace Foundation is also determined to promulgate the outcomes of the workshop across relevant other fora, including the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) as well as the Open-Ended Working Group (OEWG).

As cyberattacks continue to proliferate and effects become ever more palpable, it is important to join forces and re-instil trust in digital infrastructures to continue to derive economic and social benefits from them. Collaboration oriented fact-finding processes can go a long way in terms of raising the costs for nefarious actors in cyberspace and inducing more robust accountability and responsibility structures.