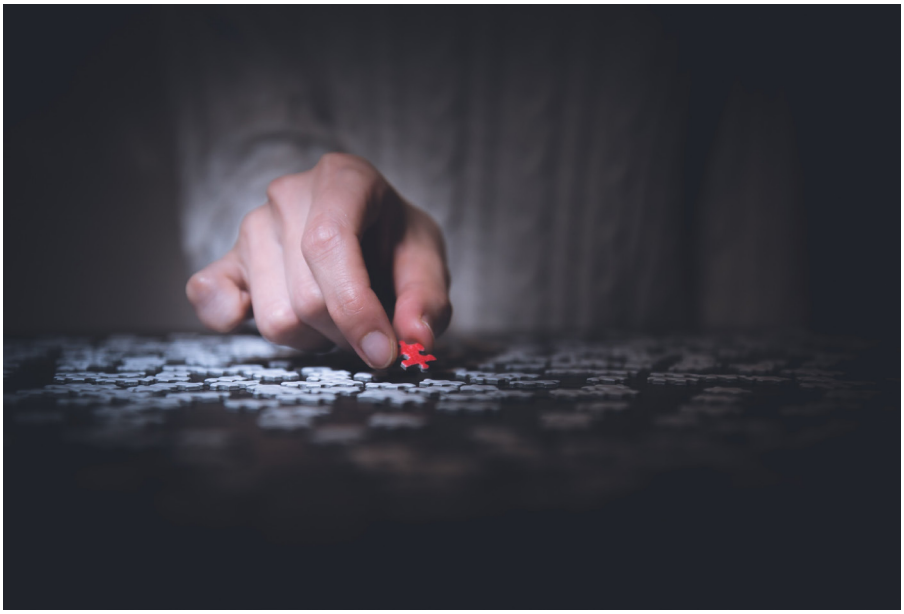
Public Attribution of Cyber Incidents

Cyber incidents are increasingly being publicly attributed to specific perpetrators. The public attributions issued by states and cybersecurity companies often lack both transparency and verifiability. Strengthening trust in public attributions requires institutional mechanisms at the international level as well as the engagement of the state, the corporate sector, and civil society.

By Florian J. Egloff and Andreas Wenger

Who did it? Identifying the perpetrators of cyber incidents has long been considered to be among the technically more demanding challenges. This remains true today. Owing to the structure of the internet, it is fairly easy for the attackers to achieve a degree of technical anonymity. This gives the attackers an advantage, since the affected party will often not know at first who carried out the attack. The multifaceted and usually time-consuming forensic search for the perpetrator is known as the attribution process. If the affected party believes they have identified the culprit, it must decide whether, and how, to react to the cyber incident. One possible course of action is public attribution, in which responsibility for the cyber incident is publicly assigned to a specific perpetrator.



Attribution processes involve multifaceted and usually time-consuming forensic searches, with the goal of identifying the perpetrator. *Ryoji Iwata / Unsplash*

For a number of years now, public attributions of cyber incidents by state authorities and corporations have been on the rise. Among the former, the US has been one of the most active states in the field of public attributions. The act of attribution may take pace in a number of ways, ranging from public statements and lawsuits to joint communiqués with coalition partners. On the corporate side, it is mainly cybersecurity companies that attribute cyber incidents to specific perpetrators in publicly accessible reports. Moreover, some companies go so far as to hold certain states directly responsible for the actions of these perpetrator groups.

Both modes of public attribution are politically significant for democracies in particular. Public knowledge about digital interactions between attackers and victims is a prerequisite for democratic decisionmaking and therefore essential for the political legitimacy of the available courses of action – ranging from insurance matters and criminal proceedings to questions of war and peace – both nationally and internationally. A lack of transparency and accountability means that societies are left in the dark as to how and why states and cybersecurity companies reach the conclusions that they communicate to the public. Proposals for international governance and

confidence-building on attribution processes show that states, corporations, and civil society – including universities – must all play their part in mounting a more effective response to cyber incidents.

Political Legitimacy

Political legitimacy in democracies is geared towards making government actions transparent. In the field of cybersecurity, therefore, a minimum of public attribution is necessary for ensuring transparency of governmental action. While preventive and passive countermeasures can be undertaken to boost one's own cybersecurity even without knowledge of potential offenders, a response to specific attackers requires the ability to determine who was responsible for the incident. If this information is available, the question arises as to whether the insights gained should be communicated to the public.

This question will be answered in different ways in different political systems. In terms of domestic politics, when it comes to legitimation of coercive countermeasures (criminal prosecution, war), democracies find themselves compelled to foster transparency more often than autocracies do. However, even democratic polities will avoid public transparency as long as cyber conflicts are seen as part of an ongoing confrontation primarily between intelligence agencies. Due to the Janus-headed nature of all state actors in the field of cybersecurity, where they appear both as protectors and as perpetrators, public attribution of cyber incidents is a matter of extreme political sensitivity. The differences between various political systems in terms of domestic disputes over threat politics create potential avenues of attack for authoritarian states in particular – although given the interconnectedness of technical systems, the strategic outcomes of such actions are hard to control for all parties involved.

It is against this background that the observable strategic restraint of state actors in consciously deploying cyber operations for coercive purposes must be understood. On the one hand, on the international level, the aim is to maintain a minimum of strategic stability. In this context, the ability to attribute cyber incidents is critical; the absence of such a capability jeopardizes traditional security mechanisms. Deterrence and escalation control are predicated on the assumption that the responsible perpetrators can be identified and countermeasures taken. On the other hand, the capability for plausible public attribution is also a precondition for international cooperation in cyberspace. If cyber norms are to establish the framework for responsible action in cyberspace, the adherence to or violation of such norms must be observable by other actors. In such a situation, public attribution may serve as a means of proscribing norm violations.

Asymmetry of Knowledge

Public attributions of cyber incidents have increased in recent years. At the state level, cybersecurity has become a core topic of security policy. States have increasingly oriented their intelligence services towards this issue and invested in attribution capabilities. At the same time, public attribution as a course of action has become part of the repertoire of policy responses in foreign and security policy. In the corporate sphere, too, attribution capabilities have developed rapidly. New technical means have been developed in the field of cyber forensics, together with new methods of identifying culprits. Today, cybersecurity businesses routinely publish reports on Advanced Persistent Threats (APTs), i.e., professional hacker groups that act continuously and with high resource intensity against their victims in a targeted manner.

> The capability for plausible public attribution is a precondition for international cooperation in cyberspace.

However, only few state and private actors have at their disposal the professional attribution processes and capabilities required to identify those actors that are politically responsible for cyber incidents. These are mainly the states with powerful signals intelligence (SIGINT) capabilities as well as a few select corporations that operate their own global sensor networks or whose business model gives them insight into global data flows. Most other state and private actors have neither the capability to attribute themselves, nor the financial resources to purchase that attributive capacity. Concerning the political legitimacy of truth claims associated with public attributions, this asymmetry of knowledge is problematic. Knowledge that is not independently verifiable is subject to political manipulation – by those in the know, but also by the ignorant.

Lack of Transparency

Public attributions of cyber incidents by states and cybersecurity companies often lack transparency. The allocations of blame cannot be verified in detail based on the published information. On the one hand, this reflects the absence of any established international standards on attribution. Internationally approved forensic techniques have yet to be fully established. On the other hand, there is often more agreement among experts than the public is aware of. This, in turn, is due to structural factors that encourage states and companies to withhold parts of the available information in their communications with the public.

In the politics of cybersecurity, states must weigh several interests against each other: They have both offensive and defensive means at their disposal and are uncertain as to the motives and capabilities of their competitors. In spite of strategic restraint, they are directly or indirectly responsible for a large part of offensive actions carried out in cyberspace. When confronted with cyber incidents, due to structural incentives for states, the secrecy of technical capabilities and sources remains the default response to cyber incidents. Public attributions remain the exception. If cyber incidents are publicly attributed to specific perpetrators, there are always manifold political reasons for doing so. So far, most public attributions have appeared to be related to foreign and security policy interests. However, to a lesser extent, they may also serve the pursuit of domestic interests.

Cybersecurity companies, on the other hand, have an interest in publicly demonstrating their independent analytical capabilities. Their reports are important channels for gaining publicity in a growth market. At the same time, however, they also have sound structural motivations not to provide insight into all of their data sources. First, the data accumulated by a cybersecurity company constitutes a trade secret of considerable commercial value. Second, the best data is often extracted from customer networks that are subject to confidentiality agreements. Third, cybersecurity firms have only limited insight into cyber conflicts based on the technology they offer and the markets in which they are active. Overall, this means that cybersecurity companies have detailed knowledge on a limited number of actors, with only a small part of that knowledge making its way to the public.

The Process of Attribution

Attribution is an inherently interdisciplinary activity. In case of cyber incidents, it requires a solid grounding in computer science, especially in the fields of forensics, network security, and malware analysis. However, other fields of knowledge, including political science, economic science, psychology, administrative science, and law, also have important contributions to make, both to the process of attribution and to an understanding of public attributions.

In the attribution process, knowledge is generated about the origins of a cyber incident. Analytically, this process can be structured into three levels. At the tactical level, the investigation aims to establish what exactly happened and how it was done. At the operational level, additional insight on the perpetrator is adduced based on the totality of available intelligence sources. Finally, at the strategic level, the incident is assessed politically. Here, one of the aims is to contextualize the reason for the event in terms of other incidents. The process concludes with a determination as to whether any political consequences must be drawn from the incident, and if so, which ones. At this point, public attribution is only one of many possible courses of action.

Different actors are involved at each of the three levels. On the tactical level, states, companies, or private individuals hire the services of cybersecurity companies that specialize in incident response. Public authorities mainly become involved when there is a link to national security or an emerging criminal case. At the operational level, attribution processes mainly come under the purview of the intelligence services, though in the context of criminal proceedings, they may also be handled by the police or the public prosecutor's office. At the strategic level, the available courses of action are usually formulated by members of the national security staff. They deliver comprehensive assessments of cyber incidents, situating them in the larger foreign and security policy context. Accordingly, courses of action are not limited to cyberspace and may include the full range of available political instruments.

Institutional Mechanisms

At the international level, there is no institutionalized mechanism for public attribution in the field of cybersecurity. However, recently, increasing demands for such a mechanism have been voiced. As of yet, there is no consensus regarding which actors should become involved in which way in an international attribution process. A vast range of suggestions has been proposed regarding the degree of involvement of states, companies, and civil society actors, the nature and context of cyber incidents as well as the organizational form and the binding nature of such regulations. For the credibility of public attributions, what matters is which actors – at the industry, state, or civil society level – are at the center of the proposed measures.

Industry-centric approaches focus on the attribution of state-sponsored cyber incidents, which may run contrary to the interests of global corporations. In 2017, for example, *Microsoft* proposed establishing an independent organization to facilitate cooperation between technology companies in the sphere of attribution. The primary goal of such an organization would be the capability to identify and categorize cyber incidents emanating from state actors in a politically neutral fashion. *Microsoft* hopes that international cooperation among cybersecurity experts as well as transparency on data and conclusions can help bridge the deficit of trust that public attributions must currently overcome.

State-centric approaches also focus on the attribution of cyberconflicts between states. One example is the proposal by a Russian think tank to establish an independent cyber-court (of arbitration) for cyber conflicts between states. A similar position has been adopted by the US think tank *Atlantic Council*, which has recommended a multilateral adjudication body for cyber incidents above the threshold of armed conflict. States with advanced attribution capabilities would make these available to the proposed forum, while states lacking such capabilities could bring their cases before the body. The forum would pass on evidence or recommendations to international or regional security organizations, which would have the final say on possible sanctions.

At the international level, there is no institutionalized mechanism for public attribution in the field of cybersecurity.

A number of approaches rooted in civil society have also been introduced. *AccessNow* criticizes the excessive emphasis on the establishment of new organizations. Instead, the NGO suggests that more emphasis be placed on the development of guidelines and evidentiary standards. Ronald J. Deibert, director of the *CitizenLab* in Toronto, has tabled the idea of a network of university institutes that could carry out distributed, transparent, peer-reviewed research on cyber incidents. A different approach is proposed by the *RAND Corporation*, another US think tank, which recommends a standing global consortium of non-state actors focused on attribution of the most significant cyber incidents.

All of these recommendations aim to reduce the asymmetry of knowledge in the sphere of public attribution and to counteract the attendant distrust toward public attributions. They all assume that public attributions will be trusted if they are reviewed transparently by an international network of experts.

However, from a political point of view, it makes a difference whether incidents are state-sponsored or not. In case of cyber conflicts at the state level, any political response requires the involvement of public actors, while non-state incidents only require an exchange between states. Accordingly, a network of international mechanisms is needed that features mutually complementary state-based, corporate, and civil-society-centered approaches. Attribution capabilities are established in a decentralized manner and based on structures of

Further Reading

Deibert, R. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs, 32* (4), 411–424. *CitizenLab* also researches the topic of targeted cyberattacks against civil society.

Grindal, K., Kuerbis, B., Badiei, F., & Mueller, M. (2018). Is it time to institutionalize cyber-attribution? *Internet Governance Project White Paper.*

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies, 38* (1–2), 4–37.

Schulzke, M. (2018). The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty. *Perspectives on Politics, 16* (4), 954–968.

The US government has provided some transparency regarding its methods of attribution in: Office of the Director of National Intelligence (ODNI) (2018). "A Guide to Cyber Attribution". *U.S. Office of the Director of National Intelligence Publication.*

trust both national and regional, state and non-state. When considering the political response, the matter of sanctions, and international stability, however, it is mandatory that these decentralized structures should be linked up with existing regional and global security institutions.

The Role of Universities

Developing a viable framework of governance for public attribution of cyber incidents requires the involvement of state, corporate, and societal actors. Universities, too, can play an important confidence-building role in this connection. They elaborate and communicate public, transparent, peer-reviewed knowledge and can thus also counteract the asymmetry of knowledge in the sphere of public attribution of cyber incidents, as outlined above. As such, they can make two distinct contributions: research and networking.

On the one hand, universities can conduct interdisciplinary and peer-reviewed research on the problem of attribution. Studying the processes of public attribution requires a pooling of technical, organizational, and political expertise. Basic research can supply the foundation for building and verifying international evidentiary standards. Research can explain how evidentiary standards and norms come into existence in practical attribution work. Moreover, research can help explain how international mechanisms of public attribution and the related governance networks can be designed to ameliorate the trust deficit.

> Universities, too, can play an important confidence-building role in this regard.

On the other hand, universities can also contribute to the study of digital conflicts. University labs that have their own interdisciplinary attribution expertise and access to independent data collection could research the multilayered realities of cyber conflicts. A network of university institutions, conjoined in a consortium, could considerably expand the body of public knowledge surrounding these societally and politically relevant questions. Building up interdisciplinary knowledge in the field of attribution and anchoring that knowledge in the training of the next generation of analysts is indispensable for gaining a better understanding of conflicts in the digital domain.

Dr. Florian J. Egloff is a Senior Researcher in Cybersecurity at the Center for Security Studies (CSS) at ETH Zurich and a Research Associate at the Centre for Technology & Global Affairs at the University of Oxford.

Prof. Dr. Andreas Wenger is Professor of International and Swiss Security Policy at ETH Zurich and Director of the Center for Security Studies (CSS) at ETH Zurich.

CSS Analyses is edited by the Center for Security Studies (CSS) at ETH Zurich. Each month, two analyses are published in German, French, and English. The CSS is a center of competence for Swiss and international security policy.

Editors: Lisa Watanabe, Fabien Merz, Benno Zogg
Layout and graphics: Miriam Dahinden-Ganzoni
ISSN: 2296-0244; DOI: 10.3929/ethz-b-000340841

Feedback and comments: analysen@sipo.gess.ethz.ch
More issues and free online subscription:
www.css.ethz.ch/en/publications/css-analyses-in-security-policy