An attribution organization to strengthen trust online

Microsoft Policy Papers

Establishing an International Cyberattack Attribution Organization to strengthen trust online

Today's digital world depends on people, businesses and governments trusting in technology and in the systems that protect them. If someone steals or damages physical property, investigators can collect evidence and involve the courts. In the digital world, the evidence of cyberattacks is often spread across technology providers, telecom operators, and victims. That evidence can also be highly technical, with only a limited number of experts in either the public or private sectors that can find it and analyze it. Furthermore, if it is a government behind the cyberattack then the challenge of proving their responsibility becomes all the more complex.

The world needs a new form of cyber defense. An organization that could receive and analyze the evidence related to a suspected state-backed cyberattack, and that could then credibly and publicly identify perpetrators, would make a major difference to the trust in the digital world. It would also give governments a legitimate basis to take further action against the perpetrators. The technology sector should work with supportive non-profit groups, to create such an organization and help deter nation state attacks in cyberspace.

Organized cooperation between technology companies can advance attribution

The expertise of private sector technology firms should be the basis of this non-political, technically-focused attribution organization. The ability of private sector technology firms to collect and analyze data from cyberattacks has improved dramatically in recent years. Online service providers and security researchers are now able to identify some cyberattacks launched by states or state-sponsored proxies. Enabling these firms to collaborate and to combine and compare data, through an attribution organization, would strengthen public trust in attribution.

The attribution organization should be a non-governmental and primarily made up of experts in cyber-forensics and related disciplines, who can analyze the technologies and techniques of a cyberattack. They can ensure that evidence related to particular attacks is gathered and presented in a way that is suitable for use by government experts and to be understood by the public. The proposed organization should also have a mechanism to work with government experts, as needed, although governments would have no power to veto a final report.

Agreements between the attribution organization and private sector firms to collect and share data will be critical. In-depth knowledge of methods used can be derived from cyberattacks, particularly as they accumulate over time. This information will enable the organization to understand attackers' behaviors and identify responsible parties with increasing certainty.

Independence, transparency and diverse geographic representation will be essential

Trust in the attribution organization amongst governments, businesses and citizens is essential if it is to do its job. It will have to be staunchly politically-neutral and focused on concrete facts and data. The organization absolutely cannot take sides or be influenced by political agendas.

In order to succeed, the organization will also have to be transparent. A robust peer review process will be required to ensure its findings are examined and confirmed by other cybersecurity experts. Its data and findings will have to be shared with the international community.

The focus must be attribution of major infrastructure attacks, not incident response or enforcement

The attribution organization should not be an incident response center providing recovery support services. A number of public and private sector groups, such as Computer Emergency Response Teams, already fulfil this role. Instead, the primary purpose of the organization will be to identify and attribute state or state-sponsored cyberattacks and present technical evidence to governments, enterprises, and the public.

Given the sheer number of cyberattacks that occur daily, the organization should only focus on the most significant ones. A threshold for the attacks that will be accepted for analysis and attribution will need to be established. Fundamentally though, the organization should focus on attacks that target critical infrastructures (e.g., power and water utilities), important elements of the global economy (e.g., underpinnings of the financial systems such as clearing or settlement), or core mechanisms of the internet (e.g., domain name servers).

Equally, the attribution organization will only be responsible for the identification of attackers. It will be the job of governments to determine what the appropriate political and diplomatic responses should be and to action them.

A trusted attribution organization is key and work is now underway to help create it

The need for an attribution organization clearly exists today. This is demonstrated by both the increasing frequency and sophistication of cyberattacks, as well as growing government insecurity, which is driving heightened cybersecurity policy activity and investments in offensive cyber capabilities. Yet, when states allege that geopolitical rivals have targeted them, there is no organization that can present a politically-neutral and fact-based analysis.

Accountability must follow attribution, and nation-states will ultimately have to determine how to act on the group’s findings. However, an independent and trusted source of attribution would provide the foundation for a fact-based, global dialogue about the nature of significant cyber-attacks. At the same time, accurate attribution would put pressure on governments to exercise restraint.

There are several possible models for an international cyberattack attribution organization. The characteristics of being private sector-led, independent and transparent, and with a singular focus on attribution are almost certain to be essential to the organization being both effective and trusted. The model and operation of the organization is where further debate across different stakeholders needs to occur in the weeks and months to come.