An attribution organization to strengthen trust online
THE WORLD NEEDS A NEW FORM OF CYBER DEFENSE—AN ORGANIZATION THAT CAN RECEIVE EVIDENCE, ANALYZE IT, AND IDENTIFY BAD ACTORS

Establishing an international cyberattack attribution organization to strengthen trust online

The future stability of our digital society depends on our ability to retain people’s trust in technology.

In the physical world, when someone steals or damages property, a neutral party (the police) collects the evidence and refers appropriate cases to the courts.

In the cyber world, when it is suspected that a government is involved in stealing information or damaging systems, the evidence is often spread among cloud providers, telecom providers, and the victims.

Additionally, it is often private computer security experts who know how to find and analyze the evidence, much of which is highly technical.

The world needs a new form of cyber defense—an organization that can receive all this evidence, analyze it, and credibly and publicly identify bad actors, thus permitting governments to take further action.

This type of transparency and accountability is essential, especially for significant attacks in which nation-states are the suspected culprit.

The technology sector should work together, and work with supportive nonprofit groups, to create an organization that would leverage its attribution capabilities to better deter nation-state attacks in cyberspace.

Organized cooperation between tech 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 primarily made up of private sector experts in cyber forensics and related disciplines, who can analyze the technologies and techniques of a cyberattack. Their research and analysis could be underpinned by powerful analytics tools made possible by cloud technologies.

They can ensure that evidence related to particular attacks is gathered and presented in a way that is suitable to be used by government experts and to be understood by the public.

The proposed attribution 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.

Information that can be derived from cyberattacks, particularly as it accumulates over time, and in-depth knowledge of methods used in different attacks will enable the organization to understand attackers’ behaviors and identify responsible parties.

**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 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, because a number of public and private sector groups, such as Computer Emergency Response Teams, already fulfill 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, and increasing government
insecurity, manifested in heightened
policy activity and investments in offensive
cyber capabilities.

Yet, when states allege that geopolitical
rivals have targeted them, there is not a
neutral 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. Microsoft is currently
looking at many different models for
a functional international cyberattack
attribution organization.

The characteristics of being private
sector-led, independent, transparent,
and a singular focus on attribution are,
according to early research, essential
to the organization being both effective
and trusted.

Microsoft has partnered with RAND, a
policy think tank, to develop this work
further and will bring forward a range
of potential models for an attribution
organization in the coming months.