CYBERATTACK ATTRIBUTION

A BLUEPRINT FOR PRIVATE SECTOR LEADERSHIP

RESEARCH FELLOWS
Justin Collins
Cameron Evans
Chris Kim
Kayley Knopf
Selma Sadzak
Nicholas Steele
Julia Summers
Alison Wendler

SENIOR RESEARCH FELLOWS
Allison Anderson
Stacia Lee

FACULTY LEAD
Jessica Beyer
This report is a product of the Applied Research Program in the Henry M. Jackson School of International Studies at the University of Washington. The Applied Research Program matches teams of top-achieving Jackson School students with private and public sector organizations seeking dynamic, impactful, and internationally-minded analyses to support their strategic and operational objectives.

For more information about the Applied Research Program please contact us at jsisarp@uw.edu.
Executive Summary

After three decades of development, adoption, and innovation, the Internet stands at the core of modern society. The same network that connects family and friends across the world similarly ties together all aspects of daily life, from the functioning of the global economy to the operation of governments. The digitization of daily life is the defining feature of the 21st century. While the pervasiveness of Internet-enabled technology brings significant benefits, it also brings serious threats—not only to our economy and safety, but also to our trust in computer systems.¹

The Internet is central to modern life, yet major state-sponsored cyberattacks persist in disrupting Internet access and function. These attacks undermine faith in government and public trust in democratic institutions. Attribution attempts to date have been unable to deter states from building malicious code for even greater destructive capabilities.

In response, we propose the formation of an attribution organization based on international private sector coordination. Drawing upon private sector expertise from multiple countries, the proposed organization will centralize analysis of major cyberattacks through formalized investigations and the production of a credible, timely attribution report following major attacks. The organization will streamline the attribution process, thereby playing a substantial role in deterring future major nation state cyberattacks and promoting greater global Internet security.

The Attribution Challenge

Attribution is critical to the resolution of many cybersecurity problems.² Attribution is important for two key reasons. First, attribution imposes responsibility on the party or parties involved in the cyberattack. Second, attribution deters future cyberattacks by raising the cost of state-sponsored offensive activity.³ Despite the tendency for countries to employ cybersecurity policy that favors offensive action rather than defensive action, attribution is fundamental to deterrence because it raises the cost of attack. Currently, attackers are predominantly anonymous, able to hide behind complex computer networks. Lack of attribution is a principal cause for the deluge of state-sponsored cyberattacks because it makes offensive cyber activity relatively cost-free.⁴

While the need for attribution is clear, speed and integrity are key obstacles to the production of successful attribution judgements.\textsuperscript{5} Evidence is paramount to the production of a credible attribution judgement; after a cyberattack, experts must gather technical and socio-economic and political data. These data become the evidence required for an attribution judgement, resolving the basic question of cyberattack responsibility.\textsuperscript{6}

However, since cyberattacks often transcend borders, divergent legal frameworks and different state strategic orientations towards information sharing make the collection of evidence particularly difficult and slow.\textsuperscript{7} Meanwhile, the integrity of digital forensics vanishes quickly. Additionally, expert investigators from the private sector lack the ability to collect necessary information from attacked governments and other companies. As a result, when attribution reports are made, they are often unconvincing to the public.\textsuperscript{8} There is clearly a need for the formal coordination of stakeholders to share, process, and publish a timely attribution judgment following major cyberattacks.

Blueprint for an Attribution Organization

The mission of our proposed attribution organization is to enhance the credibility, speed, and accuracy of attribution following cyberattacks. The organization will accomplish its objectives through private sector cooperation and funding.

To create an effective organizational blueprint, we studied 23 existing attribution organizations and investigative processes. Drawing upon the successful procedures of existing organizations and processes will enable our proposed organization to centralize analysis of major state-sponsored cyberattacks and safeguard trust in technology.


The processes we examined were: Cheonan Joint Investigation Group, Democratic National Committee Email Leak Investigation, Google’s Operation Aurora, the Intermediate-Range Nuclear Force Treaty investigative process, Malaysia Airlines Flight 17 (MH17) Crash

\textsuperscript{7} Carlin, 2016.
\textsuperscript{8} Schneier, 2015.
Investigation, Mandiant’s APT1, Mumbai Terrorist Attack Investigation, Sony Pictures Hack Investigation, and the Stuxnet Investigation.

Based on our research, we have identified six best practices to incorporate into our attribution organization:

- Equitable geographic representation
- Organizational transparency
- Stakeholder outreach
- Internal accountability
- Inclusion of technical and geopolitical experts
- Private sector membership

In addition, we articulated seven challenges that might accompany organizational operation:

- Earning public trust
- Cooperation among competitors
- Industry compliance with organizational norms
- Legal challenges of information sharing
- Collecting sensitive and confidential cyber incident information
- Methods of information sharing
- Sharing information with China and Russia

Our report details each of the listed best practices and outlines how each practice will be integrated into an organization tasked with cyberattack attribution. We also address each potential challenge and propose solutions that will promote international cooperation and enhance global Internet security.

Table 1 illustrates our organizational blueprint. As a non-governmental organization funded entirely by private sector members, the organization will derive its legitimacy and authority from its reputation for neutrality, transparency, and stringent evidentiary requirements. The organization will also incorporate transparent decision-making processes, including use of Executive Council supermajority voting procedures prior to publishing attribution judgements, expert-led investigation committees, and peer review of findings through expert review committees. The organization will disseminate attribution judgements to a variety of media outlets, rather than being announced by an individual government or given exclusively to one news organization.
Table 1: Organizational Blueprint

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>Company representatives, industry experts, independent academics</td>
</tr>
<tr>
<td>Actions</td>
<td>- Leads neutral, private sector investigations of major state-sponsored</td>
</tr>
<tr>
<td>-</td>
<td>cyberattacks to determine attribution.</td>
</tr>
<tr>
<td>Authority</td>
<td>- Reputational</td>
</tr>
<tr>
<td>Structure</td>
<td>- Decision making done through supermajority voting of member companies in the</td>
</tr>
<tr>
<td>-</td>
<td>Executive Council</td>
</tr>
<tr>
<td>-</td>
<td>Expert Investigation Committee leads nation-state cyberattack investigations</td>
</tr>
<tr>
<td>-</td>
<td>Expert Review Committee reviews validity of attribution judgment upon</td>
</tr>
<tr>
<td>-</td>
<td>request</td>
</tr>
<tr>
<td>Norms</td>
<td>- Peer-review, high transparency, evidentiary framework</td>
</tr>
<tr>
<td>Attribution</td>
<td>- Investigation report articulates attribution</td>
</tr>
<tr>
<td>-</td>
<td>The Communications Committee disseminates attribution report, with full</td>
</tr>
<tr>
<td>-</td>
<td>transparency, to mainstream news organizations</td>
</tr>
<tr>
<td>Budget and Funding Source(s)</td>
<td>- $40 million for year one and $30 million/year for subsequent years</td>
</tr>
<tr>
<td>-</td>
<td>Funded by mandatory contributions from member companies</td>
</tr>
</tbody>
</table>

Figure 1, below, captures the direction of information flow. As the figure illustrates, information arrives at the organization through an information repository. As evidence is collected, an Expert Investigation Committee verifies the veracity and authenticity of the evidence. An Expert Review Committee also examines the evidence and the findings of both groups create the substance of the attribution report. The Expert Review Committee disseminates the attribution report to the Communication Committee. The Communication Committee works with the media to publicize the results of the review.

Figure 1 also illustrates the organization’s authority and accountability hierarchy. Member companies populate an Executive Council of Company Representatives and a Budget Committee. The Executive Council provides resources and oversight to the two experts groups. It also assists with the dissemination of the organization’s findings. The Executive Council members serve under four-year term limits. Term limits are incorporated into the Executive Council’s design as a governance mechanism to ensure diversity within the executive leadership.
Figure 1: Organizational Chart

The proposed organization will have the ability to provide widely legitimate attribution judgements following major cyberattacks. Diversity of membership and procedural transparency will bolster the organization’s reputational authority, while the coordination of a global body of technical experts will lead a neutral investigation of attacks. A private-sector led attribution organization will centralize and optimize the attribution process, thereby holding parties responsible for cyberattacks while increasing the cost of perpetration. Such an organization will ultimately foster improved global cybersecurity.
Table of Contents

Executive Summary ........................................................................................................................................... i
The Attribution Challenge ................................................................................................................................. i
Blueprint for an Attribution Organization ...................................................................................................... ii

Table 1: Organizational Blueprint ................................................................................................................... iv
Figure 1: Organizational Chart ......................................................................................................................... v

Introduction ..................................................................................................................................................... 1
Blueprint for an Attribution Organization ..................................................................................................... 3

Table 1: Organizational Blueprint ................................................................................................................... 5
Figure 1: Organizational Chart ......................................................................................................................... 7
Figure 2: Incorporation of Best Practices ......................................................................................................... 8

Creating A Cyberattack Attribution Organization .......................................................................................... 9
Mission ............................................................................................................................................................. 9
Methodology .................................................................................................................................................... 11

Actors. ............................................................................................................................................................. 12
Actions............................................................................................................................................................. 12
Authority. ......................................................................................................................................................... 12
Structure.......................................................................................................................................................... 12
Norms. ............................................................................................................................................................. 12
Attribution. ....................................................................................................................................................... 12
Budgeting and Funding Sources ....................................................................................................................... 12

Figure 3: Spectrum of State Authority ............................................................................................................. 13

Incorporating Best Practices .......................................................................................................................... 14
Equitable Geographic Representation ................................................................................................................ 14

Equitable Geographic Distribution: Greenpeace, OPCW, and the Cheonan Joint Investigation Group........... 15
Adopting Equitable Geographical Representation .......................................................................................... 16

Organizational Transparency .......................................................................................................................... 16

Low Transparency Model: The Cheonan Joint Investigation Group ............................................................... 17
High Transparency Model: Mandiant’s APT1 Report ......................................................................................... 19
Adopting Transparency ................................................................................................................................... 20

Stakeholder Outreach ..................................................................................................................................... 20

Stakeholder Outreach Models: OPCW and the Egmont Group ................................................................... 21
Adopting Stakeholder Outreach ....................................................................................................................... 22

Internal Accountability .................................................................................................................................... 22

Internal Accountability Models: UN ISIL and al-Qaida Sanctions Committee and the INF Treaty............ 23
Adopting of Internal Accountability ................................................................................................................ 23

Inclusion of Technical and Geopolitical Experts ............................................................................................ 24

Expert Inclusion Models: The Cheonan Investigation and the IAEA ............................................................. 24
Adopting Expert Inclusion in Investigations.................................................................................................... 25
International Atomic Energy Agency (IAEA) .............................................................................................................. 62
International Civil Aviation Organization (ICAO) ........................................................................................................ 63
International Labor Organization (ILO) ....................................................................................................................... 64
NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) .............................................................................. 65
Organization for the Prohibition of Chemical Weapons (OPCW) ............................................................................. 66
United Nations Al-Qaida Sanctions Committee ........................................................................................................ 67
United Nations Sanctions Committee on North Korea ................................................................................................. 68
World Trade Organization (WTO) GATT Article XX ................................................................................................. 69

Appendix 2: Investigative Processes ............................................................................................................................... 70
Cheonan Joint Investigation Group (JIG) ........................................................................................................................ 71
Democratic National Committee (DNC) Email Leak Investigation ............................................................................... 72
Google’s Operation Aurora .............................................................................................................................................. 73
Intermediate-Range Nuclear Force (INF) Treaty Investigative Process ........................................................................ 74
Malaysia Airlines Flight 17 (MH17) Crash Investigation .............................................................................................. 75
Mandiant’s APT1 ............................................................................................................................................................. 76
Mumbai Terrorist Attack Investigation .......................................................................................................................... 77
Sony Pictures Hack Investigation ..................................................................................................................................... 78
Stuxnet Investigation ......................................................................................................................................................... 79

Appendix 3: Proposed Budget ............................................................................................................................................ 80
   Table 2: Proposed Budget for Year 1 and Subsequent Years ....................................................................................... 81

Bibliography .................................................................................................................................................................... 82
Introduction

In April 2007, Estonia was cut off from the Internet.\(^9\) For three weeks, a series of coordinated botnet attacks flooded the country’s Web, email, and domain name system servers. The distributed denial-of-service attack seemed like a concerted effort to protest Estonia’s removal of a Soviet era monument in Tallinn, its capital city. One observer likened the attack to “Web War One.”\(^10\) The surprise attack had a profound impact on Estonia’s critical infrastructure, disrupting government communications as well as financial institutions, universities, and media.

Although the Estonian government accused Russia of the cyberattack, the extent to which the Russian government actively supported the attackers remains a mystery.\(^11\) Failure to conclusively identify the perpetrators of the Estonia attack marked a turning point in the nature of cyber warfare, signaling to states that offensive cyber activity can be risk-free. Without definitive attribution, the outcome of the Estonian attack emboldened future attackers.

The Estonian case illustrates the challenges of cyberattack attribution. Not only does the anonymity of the Internet mask attackers, gathering digital evidence to identify an attacker is difficult. Accumulating evidence also takes time, creating space between the attack and any attribution, which contributes to the ambiguity over who the attacker is and what their motives are. Governments’ and companies’ inability to consistently identify bad actors has meant that reliable attribution has remained intangible.

While ordinary Internet users may have a restricted understanding of cybersecurity, attackers are both indiscriminate in selecting victims and thoughtful in choosing targets that advance

---


nation state goals. In both cases, they capitalize upon the Internet’s ever-expanding number of vulnerabilities. In the past few years alone, Russia has infiltrated the emails of the Democratic National Committee and China has supported so-called “Advanced Persistent Threats” in stealing billions of dollars of trade secrets and other sensitive data from corporations. These political and personal risks will only multiply in the future, as Internet of Things technology expands to connect an unprecedented number of devices across the world.\(^\text{12}\)

Attribution, or the identification of an attacker, is a challenge at the core of many cybersecurity problems.\(^\text{13}\) Due to the complex nature of cyberattacks, where sophisticated attackers often use network computers to carry out malicious activity, attribution refers to a spectrum of identification. The spectrum can range from the proxy computer, to the individual culpable of “pressing the key,” to the nation state sponsoring the hackers.\(^\text{14}\) One goal of attribution is to answer who was really behind the attack. Another goal is to deter future attacks by raising the cost of the activity.\(^\text{15}\)

Despite the current tendency for nation state cybersecurity to favor offensive action over defensive action, attribution is fundamental to deterrence because fear of retaliation could dissuade attacks.\(^\text{16}\) The attacker’s invisibility is a principal cause for the deluge of cyber threats because it makes his or her actions relatively cost-free.\(^\text{17}\)

Therefore, attribution raises the cost of hacking. Confidence in attribution is determined by the strength of evidence drawn on several dimensions—technical forensics, human intelligence,


\(^{15}\) For more on this see: Jon R. Lindsay, “Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack.” *Journal of Cybersecurity* 1, no. 1 (September 1, 2015): 53–67. [http://cybersecurity.oxfordjournals.org/content/1/1/53](http://cybersecurity.oxfordjournals.org/content/1/1/53)

\(^{16}\) Clark and Landau, 2011.

signals intelligence, and geopolitics.\textsuperscript{18} With this information, experts can produce an attribution judgment resolving the basic question of responsibility.\textsuperscript{19} Yet compounding the technical challenges of determining responsibility are nation state legal barriers preventing victims and the relevant security communities from investigating thoroughly. The Internet and multinational corporations alike bypass sovereign borders, problematizing the laws governing the collection of evidence and information sharing.\textsuperscript{20}

Government and industry responsibility surrounding attribution is currently unclear. For instance: Who is responsible for investigating cyberattacks? What role should the government and industry play in collecting evidence? What is the acceptable threshold of evidence required to make an attribution judgement? Without answers, deterrence is undermined. Our report steps into this gap, addressing these key questions, and proposes a new organization based on the successes of existing attribution organizations and processes.

\textbf{Blueprint for an Attribution Organization}

The mission of our proposed attribution organization is to enhance the credibility, speed, and accuracy of attribution following cyberattacks. The organization will accomplish its objectives through private sector cooperation and funding.

To create an effective organizational blueprint, we studied 23 existing attribution organizations and investigative processes. Drawing upon the successful procedures of existing organizations and processes will enable our proposed organization to centralize analysis of major state-sponsored cyberattacks and safeguard trust in technology.

The organizations we evaluated were (Appendix 1): Amnesty International, Citizen Lab, Egmont Group of Financial Intelligence Units, European Financial Coalition Against Child Pornography, Financial Industry Regulatory Authority, Greenpeace, International Atomic Energy Agency,

\textsuperscript{18} Lin, 2016. 11.
\textsuperscript{19} Healey, 2012.
\textsuperscript{20} Carlin, 2016.

The processes we examined were (Appendix 2): Cheonan Joint Investigation Group, Democratic National Committee Email Leak Investigation, Google’s Operation Aurora, the Intermediate-Range Nuclear Force Treaty investigative process, Malaysia Airlines Flight 17 (MH17) Crash Investigation, Mandiant’s APT1, Mumbai Terrorist Attack Investigation, Sony Pictures Hack Investigation, and the Stuxnet Investigation.

Based on our research, we have identified six best practices to incorporate into our attribution organization:

- Equitable geographic representation
- Organizational transparency
- Stakeholder outreach
- Internal accountability
- Inclusion of technical and geopolitical experts
- Private sector membership

In addition, we have identified seven challenges that might accompany organizational operation:

- Earning public trust
- Cooperation among competitors
- Industry compliance with organizational norms
- Legal challenges of information sharing
- Collecting sensitive and confidential cyber incident information
- Methods of information sharing
- Sharing information with China and Russia

Our report details each of the listed best practices and outlines how each practice will be integrated into an organization tasked with cyberattack attribution. We also address each
potential challenge and propose solutions that will promote international cooperation and enhance global Internet security.

Table 1 illustrates our organizational blueprint. As a non-governmental organization funded entirely by private sector members, the organization will derive its legitimacy and authority from its reputation for neutrality, transparency, and stringent evidentiary requirements. The organization will also incorporate transparent decision-making processes, including use of Executive Council supermajority voting procedures prior to publishing attribution judgements, expert-led investigation committees, and peer review of findings through expert review committees. The organization will disseminate attribution judgements to a variety of media outlets, rather than being announced by an individual government or given exclusively to one news organization.

Table 1: Organizational Blueprint

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Company representatives, industry experts, independent academics</td>
<td></td>
</tr>
</tbody>
</table>

| Actions | - Leads neutral, private sector investigations of major state-sponsored cyberattacks to determine attribution. |

| Authority | - Reputational |

| Structure | - Decision making done through supermajority voting of member companies in the Executive Council |
| - Expert Investigation Committee leads nation-state cyberattack investigations |
| - Expert Review Committee reviews validity of attribution judgment upon request |

| Norms | - Peer-review, high transparency, evidentiary framework |

| Attribution | - Investigation report articulates attribution |
| - The Communications Committee disseminates attribution report, with full transparency, to mainstream news organizations |

| Budget and Funding Source(s) | - $40 million for year one and $30 million/year for subsequent years |
| - Funded by mandatory contributions from member companies |

Figure 1, below, captures the direction of information flow. As the figure illustrates, information arrives at the organization through an information repository. As evidence is collected, an
Expert Investigation Committee verifies the veracity and authenticity of the evidence. An Expert Review Committee also examines the evidence and the findings of both groups create the substance of the attribution report. The Expert Review Committee disseminates the attribution report to the Communication Committee. The Communication Committee works with the media to publicize the results of the review.

Figure 1 also illustrates the organization’s authority and accountability hierarchy. Member companies populate an Executive Council of Company Representatives and a Budget Committee (budget is outlined in Appendix 3). The Executive Council provides resources and oversight to the two experts groups. It also assists with the dissemination of the organization’s findings. The Executive Council members serve under four-year term limits. Term limits are incorporated into the Executive Council’s design as a governance mechanism to ensure diversity within the executive leadership.
Figure 2 outlines how the organization adopts the best practices we identified through the course of our research. While every element of the organization does not include every best practice, each element incorporates the practices most suited to its function.
The proposed organization will have the ability to provide widely legitimate attribution judgements following major cyberattacks. Diversity of membership and procedural transparency will bolster the organization’s reputational authority, while the coordination of a global body of technical experts will lead a neutral investigation of attacks. A private-sector led attribution organization will centralize and optimize the attribution process, thereby holding parties responsible for cyberattacks while increasing the cost of perpetration. Such an organization will ultimately foster improved global cybersecurity.
Creating A Cyberattack Attribution Organization

The cyberattack attribution organization’s purpose is to make prompt and accurate attribution judgments by coordinating private sector information sharing. Today, state-sponsored cyberattack attribution suffers from two chief problems: speed and integrity.\textsuperscript{21} The process of collecting and analyzing evidence is slow, and the reliability of digital forensics vanishes quickly. Public acceptance of governments’ attribution reports is undermined because their use of confidential evidence hinders transparency, while the private sector often lacks the ability to collect necessary information. As a result, even when attribution reports are created, they are unconvincing to the public.\textsuperscript{22} There is a need for the formal coordination of stakeholders to share and process data and publish an attribution judgment. An organization tasked with sharing cyber evidence and centralizing the analysis of digital forensics and information will enhance the process of attribution.

Credible attribution judgements require international, private sector coordination. Although complete neutrality is impossible to achieve, private sector membership contributes substantially to this goal. By formalizing the investigation and creation of a credible, unbiased attribution report following major cyberattacks, the organization will play a substantial role in deterring future major nation state cyberattacks.

Mission

The mission of the proposed organization is simple; it aims to enhance the neutrality, speed, and accuracy of attribution through private sector cooperation. Doing so will diminish the number of cyberattacks as the likelihood increases that nation states are held accountable for their actions.

The design of the proposed organization addresses the problem of neutrality in an attribution


\textsuperscript{22} Ibid.
investigation. The proposed organization aims to leverage the private sector’s access to critical information with a neutral and transparent investigation process. Because private companies share a mission to protect customers online and deter future state-sponsored attacks that may threaten their bottom-line, they offer a neutral investigative party. The market incentivizes company neutrality in a way that does not exist for state actors.

Safeguarding trust in technology underpins the work of this organization. The Internet stands central to modern life, and yet major state-sponsored cyberattacks persist in disrupting its access and function. Previous attribution reports were unable to deter states from building malicious code for even greater destructive capabilities. Thus, the public’s skepticism of attribution reports erodes their perception of safety online. The lack of trust emanates from the time delay between when the attack occurs and when the attribution report is published, the confidential nature of government attribution reports, and the shortage of conclusive evidence used.  

The potential for speed and accuracy stems from the centralized collection of cyberattack information, such as threat signatures for malware, Internet protocol addresses and domain names involved in cyberattacks, and descriptions of specific cyberattacks. The upshot is that the proposed organization will have the evidence and expertise to investigate a major cyberattack. When the proposed organization publishes a report, the diversity of its membership and procedural transparency will bolsters its authority. The coordination of a global body of technical experts from the private sector will lead a neutral investigation of a major state-sponsored cyberattacks.

Therefore, the mission of the proposed organization is to fulfil the need for an unbiased and transparent process for the attribution of state-sponsored cyberattacks. At the same time providing accurate attribution will protect customers and improve their confidence in industry,

---

it will increase the public's trust in the Internet. Taken together, our argument is that with enough data points, attribution is possible, but getting members to share information requires a trustworthy organization.

Methodology

In preparing a blueprint for the proposed attribution organization, we engaged in a landscape analysis of the basic structures, processes, and best practices of existing attribution organizations and processes. We analyzed the successes and failures of 23 different organizations and processes whose missions range from nuclear nonproliferation to environmental activism and the prevention of money laundering. Tables examining each of the organizations in detail are available in Appendix 1 and Appendix 2.


The processes we examined were: Cheonan Joint Investigation Group, Democratic National Committee Email Leak Investigation, Google’s Operation Aurora, the Intermediate-Range Nuclear Force Treaty investigative process, Malaysia Airlines Flight 17 (MH17) Crash Investigation, Mandiant’s APT1, Mumbai Terrorist Attack Investigation, Sony Pictures Hack Investigation, and the Stuxnet Investigation.

We focused our review on seven key elements that are central to the operation of attribution bodies. These elements are: actors, actions, authority, structure, norms, attribution, and budgeting and funding source(s). We operationalize these terms as follows:
Actors. Actors are the party or parties that compose the main bodies of an organization or investigative process. Actors carry out the organization or investigative process’s main functions. Actors come from a range of fields and backgrounds, from government officials to government agencies, academics, researchers, and private companies.

Actions. Actions are the steps that actors take to further an organization or investigation processes’ mission. The actions of an organization are the chief duties and goals the organization or investigation works to accomplish.

Authority. Authority denotes the legitimacy of judgment and power. In the organization or investigative process, authority refers to the right to exercise judgment. Authority stems from an individual’s technical or geopolitical knowledge, or an organization’s reputation.

Structure. Structure refers to the arrangement of actors within the organization.

Norms. Norms refer to expected behavioral practices of actors within an organization or investigative process.

Attribution. Attribution refers to how an organization or investigative process publishes their findings and articulates responsibility.

Budgeting and Funding Sources. The budget refers to the operational costs of organizations or investigative process. Funding refers to the source of the budget.

Our landscape analysis proved useful in identifying successful core functions of attribution organizations and considering the application of these best practices to cybersecurity. While each organization or process has its own table of data in the Appendices, Figure 3 provides an overview of the spectrum of state authority in the international organizations and investigations we surveyed. Here, state authority refers to the influence and control wielded by a government within a given organization or investigation. An increase in size and bureaucracy is a corollary of an organization or investigation’s legal authority. Thus, the number of formal treaties increase with the presence of government actors.
<table>
<thead>
<tr>
<th>Bureaucratic</th>
<th>Ad-hoc</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>International Organizations</strong></td>
<td><strong>International Investigations</strong></td>
</tr>
<tr>
<td>• Formal authority</td>
<td>• Private Enterprises</td>
</tr>
<tr>
<td>• Nonprofit</td>
<td>• Informal authority</td>
</tr>
<tr>
<td>• Member state and private funding</td>
<td>• For-profit mission driven strategies</td>
</tr>
<tr>
<td>• Ratified treaties</td>
<td>• Ad-hoc information-sharing</td>
</tr>
<tr>
<td><strong>Tools</strong></td>
<td><strong>Greater number of participants, less specific</strong></td>
</tr>
<tr>
<td>• Bilateral, multilateral treaties</td>
<td>• Fewer number of participants, more specific</td>
</tr>
<tr>
<td>• Agreements between governments</td>
<td></td>
</tr>
<tr>
<td>• Partnerships among governmental agencies and NGOs</td>
<td></td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>• IAEA</td>
<td>• Stuxnet</td>
</tr>
<tr>
<td>• UN Sanctions</td>
<td>• Mandiant</td>
</tr>
<tr>
<td>• WTO Article XX</td>
<td>• APT1</td>
</tr>
<tr>
<td>• Amnesty International</td>
<td>• DNC Hack</td>
</tr>
<tr>
<td>• NATO CCDCOE</td>
<td>• Google’s ‘Operation Aurora’</td>
</tr>
<tr>
<td>• EFCACP</td>
<td>• Cheonan JIG</td>
</tr>
</tbody>
</table>

Figure 3: Spectrum of State Authority
Incorporating Best Practices

The purpose of the proposed organization is to enhance the neutrality, speed, and accuracy of state-sponsored cyberattack attribution. To achieve this mission, the design of the proposed organization will build upon the best practices of the organizations and investigations in our landscape analysis. In this report, we define best practices as a technique or process superior to alternatives. Best practices form the organizations’ and investigations’ standard method of procedure—from collecting evidence to complying with local laws. In the following, we will detail the best practices of the reviewed organizations and investigations and explain how the proposed organization incorporates the best practices into its design. These best practices include:

- Equitable geographic representation
- Organizational transparency
- Stakeholder outreach
- Internal accountability
- Inclusion of technical and geopolitical experts
- Private sector membership

Equitable Geographic Representation

Equitable global distribution of an organization’s decision-making bodies is key for an organization’s reputation and authority. Geographically diverse membership bolsters the credibility of the organization’s mission and actions because it balances different regional perspectives. The transnational nature of cyberattacks makes this practice even more critical. Any organization tasked with global attribution faces pressure to uphold political neutrality and independence from any one country. This is particularly important when considering interactions with major powers with global agendas, such as China, Russia, and the United States.
Equitable Geographic Distribution: Greenpeace, OPCW, and the *Cheonan* Joint Investigation Group

Several of the organizations we examined exemplify the benefit of equitable geographic distribution. In the case of Greenpeace, physical brick and mortar regional branches foster greater global cooperation because they increase the organization’s ability to connect with local sources for research and information gathering purposes.\(^2\) Having a physical global presence creates an image of Greenpeace as a global actor, rather than an organization associated with any one country and allows for the organization to draw upon ideas from all parts of the globe.

The Organization for the Prohibition of Chemical Weapons (OPCW) uses the practice of equitable geographic distribution to foster greater representation and cooperation in its governing bodies. The OPCW has strict quotas for geographic representation in each of its governing bodies. For example, the Executive Council of the OPCW always has nine representatives from Africa, nine from Asia, five from Eastern Europe, seven from Latin America, and ten from Western Europe and North America.\(^2\) Their structure ensures that, in rotation, each state party has the right and opportunity to serve on the Executive Council and actively participate in the organization’s decision-making process, thereby promoting an image of an organization that is truly international and independent. Geographic diversity is also represented in the OPCW’s Scientific Advisory Board, which conducts research and inspection of chemical weapons material. Diverse geographic representation among the body’s scientists and inspectors is important for increasing the political neutrality of the organization’s investigations into chemical weapons.\(^2\)

The investigation into the sinking of the South Korean naval vessel *Cheonan* is another example of geographic inclusion. The *Cheonan* investigation was conducted by individuals and experts from diverse geographical backgrounds, signaling greater commitment to neutrality and its


ability to produce credible findings to the international community. The investigative team was formed by the South Korean government but contained experts from Australia, Canada, South Korea, Sweden, the United Kingdom, and the United States. South Korea’s deliberate internationalization of the investigation made it harder for North Korea to dismiss the accusations of the investigation being politically motivated. In this case, geographic diversity enhanced the credibility of the investigation as being politically neutral.

Adopting Equitable Geographical Representation

Ensuring geographic representation can be fulfilled through the process of proportionally allocating the number of companies sharing information within the proposed organization to the number of major cybersecurity attacks happening within that region or country over a certain period. The proportionate number of regional firms within the organizations will contribute to efficient and pertinent amount of information sharing and will ensure all regions and countries are equitably represented. Additionally, the proposed organization will have six global offices encompassing the following regions: Africa, Asia, Russia and the Commonwealth of Independent States, Europe and Middle East, Latin America, and North America.

Organizational Transparency

The proposed organization should adopt transparency as a best practice because transparency enhances an organization’s credibility. We define transparency as a behavioral norm guiding the organizations decision to disclose information. A high-degree of transparency describes the extent to which an organization discloses information to the public.

Transparency plays a key role in fostering an organization’s reputational authority. Here, reputational authority refers to the perception of an organization’s credibility. Ensuring the organizational credibility is important for the organization’s attribution reports to be

---

considered valid and for ensuring that private sector companies will join the organization.\textsuperscript{31} In the following, we will analyze two investigations where transparency played a substantial role in the public’s confidence in the attribution report. Two of the cases we examined offer examples of attribution judgements with varying levels of transparency. First, the \textit{Cheonan} Joint Investigation Group had a low-degree of transparency, and therefore, limited credibility. In contrast, the Mandiant APT1 report is a model of high-degree transparency and a high level of credibility.

Low Transparency Model: The \textit{Cheonan} Joint Investigation Group

The \textit{Cheonan} Joint Investigation Group’s attribution report is an example of an instance in which a low level of transparency created findings that were viewed as not credible. The report was met with widespread skepticism because of the investigation’s lack of transparency. On March 26, 2010, the South Korean warship \textit{Cheonan} sank near the Northern Limit Line, a \textit{de facto} jurisdictional border with North Korea, killing 46 servicemen.\textsuperscript{32} The South Korean government withheld formal indictments immediately after the sinking, although the incident heightened tensions between the two Koreas.\textsuperscript{33} To determine the perpetrator of the attack, the South Korean government launched an independent investigation tasked with the analysis of forensic evidence from the attack.\textsuperscript{34} However, the investigation’s secretive process was highly controversial, particularly among other forensic scientists and the public.\textsuperscript{35} When the final report concluded that North Korea was responsible for the attack, controversy over the validity of the expert’s forensic analysis undermined its authority. Indeed, the United Nations Security Council condemned the attack, but did not name North Korea as the aggressor, citing “deep concern” over the reports attribution.\textsuperscript{36}

\begin{thebibliography}{99}
\item\textsuperscript{32} Landler, 2010.
\item\textsuperscript{33} Landler, 2010.
\end{thebibliography}
The controversy over the Joint Investigation Group’s findings centers on the investigation’s failure to explain its analysis of evidence. The strongest critics of the investigation’s report claim the evidence of the torpedo attack was misinterpreted or fabricated, contradicting testimony from witnesses of the ship’s sinking. Forensic scientists criticized the investigation for not publishing the data used in the analysis of forensic evidence. Disclosing such information would have allowed peer-reviewers to corroborate with the investigation’s conclusion and discredit other speculations.

Subsequent research from scientists further raised the possibility that the sinking was caused by other factors. An oversight board for the South Korean military accused the investigation of analyzing information distorted by the South Korean naval leaders. Critics speculated that the reason for not disclosing information is to protect the South Korean army from liability. A South Korean government watchdog organization sent an open letter to the United Nations Security Council questioning the findings of the Joint Investigation Groups report, highlighting the problem with the investigations lack of transparency. The leader of the organization was subsequently charged with a libel suit, worsening the public trust in the political autonomy of the investigation.

The Cheonan example illustrates why attribution investigations of state-sponsored attacks should prioritize transparency and provide an open peer-review process. In this case, the skepticism from the South Korean public and criticism from scientific community suggests that the failure to share information with the public can fuel distrust and legitimate alternative...
interpretations of the attack. Providing access to forensic evidence and technical methodology would allow the public and external experts to review potential flaws in the attribution process. Such transparency can serve as part of a system of check and balances within an investigation.

High Transparency Model: Mandiant’s APT1 Report

Because openness mitigates against distrust, the Mandiant’s APT1 report offers a valuable model for gathering and sharing a transparent attribution report. The importance of Mandiant’s report comes from the breadth of evidence disclosed to the public and engagement with the press. Mandiant, an American private security firm, spent six years collecting evidence on a series of network attacks in organizations across the world. The final report accused China’s People’s Liberation Army as the perpetrator responsible. The 60-page report details the unprecedented volume, sophistication, and persistence of these attacks, calling them “APT1” or “advanced persistent threat 1.”

Mandiant’s APT1 attribution report illustrates the legitimacy derived from providing public access to data and full-disclosure evidence. For instance, the report maps the Internet protocol addresses and other digital evidence, including drawing a line from their evidence to a specific building location in Shanghai. Using 3,000 addresses and indicators, the report also identifies specific individuals responsible for launching the attacks. The report includes an analysis of the Chinese hackers, in addition to pictures of the attackers’ social media profiles.

In addition, Mandiant shared the technical tools and procedures used to gather evidence and explained in nontechnical language the method of analysis. In doing so, Mandiant bolstered

---

the credibility of its attribution judgment by allowing extensive peer-review and public discussion. Mandiant’s transparency served to bolster the report's credibility and provide actionable information to the security industry. The report’s extensive analysis of the Chinese organization responsible for the attack will likely deter similar ones in the future.

Adopting Transparency

Our case studies offer evidence that public access to information is important to the credibility of attribution organizations and that transparency measures can be built into the design of the proposed organization. Therefore, the proposed organization should adopt behavioral norms for transparency, such as the public disclosure of information and engagement with the public during the investigatory process. Doing so will lend further credibility to any investigation.

Additionally, full disclosure will provide the public access to all sources used in an attribution judgement and address the lack of trust in state-sponsored cyberattack attribution judgments. Sharing the rationale behind decision making within the technical and geopolitics expert panel will similarly act as an instrument of accountability.

In line with this, the proposed organization should produce reports that are unclassified and can undergo extensive peer-review from independent security analysts. Not only will the organization’s openness and public engagement help to deter state-sponsored cyberattacks, disclosure of evidence and forensic analysis will buttress the organization’s credibility in the public eye.

Stakeholder Outreach

Employing stakeholder industry training and outreach is another best practice the proposed organization will adopt. Industry engagement in the form of training and outreach campaigns can facilitate stronger cooperation and cohesion between multiple stakeholders and across different sectors and regions of the world. Not only can stakeholder outreach campaigns

---

bolster an organization’s public reputation, these practices also work to inform and improve industry knowledge and increase channels for the engagement of a wide variety of industry stakeholders.\textsuperscript{50} The proposed organization will adopt practices of stakeholder outreach, incorporating the models for such processes used by the Organization for the Prohibition of Chemical Weapons and the Egmont Group of Financial Intelligence Units.

Stakeholder Outreach Models: OPCW and the Egmont Group

The Organization for the Prohibition of Chemical Weapons (OPCW) successfully utilizes practices of stakeholder outreach to promote the transnational awareness of OPCW chemical industry objectives. The OPCW holds official courses at chemical industry meetings every month for relevant industry and government stakeholders. For example, in May 2017, the OPCW held courses on analytical chemistry, on how to respond to incidents of chemical warfare, as well as assistance and protection training programs.\textsuperscript{51} Included in the OPCW’s organization structure is an Advisory Board on Education and Outreach to promote the implementation of the Chemical Weapons Convention and aid national governments and chemical industry in its disarmament objectives.

The Egmont Group of Financial Intelligence Units also employs outreach and industry training measures. Like the cybersecurity industry, the Egmont Group works in an industry with diverse stakeholders, including governmental financial intelligence units, non-governmental organizations, academia, media, and the public.\textsuperscript{52} The Egmont Group’s outreach communication strategy aims to increase their organization’s effectiveness by raising understanding and support of increased information sharing and topic awareness. The Egmont Group conducts stakeholder regional meetings and technical workshops and seminars in the promotion of the Group’s mission.


Adopting Stakeholder Outreach

Our case studies offer evidence that stakeholder outreach can be central to facilitating stronger cooperation amongst multiple stakeholders who are geographically dispersed. Therefore, the proposed organization for cyber attribution should adopt similar practices of both the Organization for the Prohibition of Chemical Weapons and the Egmont Group in the establishment of its own outreach campaigns.

The proposed organization’s Executive Council should be tasked with arranging biannual industry meetings of member and non-member companies to review and analyze the proposed organization’s practices, address potential improvements for the organization moving forward, and discuss practices of private-sector information sharing. Biannual meetings across all regional industry actors could increase awareness for the organization and help incorporate date gathering and technical knowledge from non-member regional private firms. The long-term goal of the Committee’s outreach campaigns would be to foster greater global industry engagement with the proposed organization. Global industry representative’s participation in biannual meetings would help to bolsters both transnational awareness and engagement of the proposed organization’s mission.

Internal Accountability

Internal accountability is an important practice that serves to increase credibility and trust in an attribution organization’s reports and investigative processes. Accountability is fostered when an organization provides mechanisms for internal checks and balances, such as frameworks for self-assessment, dispute resolution, and peer-review. Examples of successful internal accountability creating credibility in findings can be seen in examples of the United Nations ISIL (Da’esh) and al-Qaida Sanctions Committee and the Intermediate-Range Nuclear Forces Treaty investigative process.
Internal Accountability Models: UN ISIL and al-Qaida Sanctions Committee and the INF Treaty

The United Nations ISIL (Da’esh) and al-Qaida Sanctions Committee offers an example of a successful internal accountability framework, particularly its Office of the Ombudsperson. The Office of the Ombudsperson is an independent body tasked with overseeing the appeals processes of individuals or groups believed to be unlawfully sanctioned.\textsuperscript{53} The Ombudsperson provides detailed analysis and observations on all information relevant to a sanctions appeal before providing the Committee with a recommendation on delisting.\textsuperscript{54} The Office of the Ombudsperson helps to strengthen the Committee’s position against complaints of violating the legal rights of sanctioned individuals and is an important step in enhancing fairness and transparency within the sanctions regime.\textsuperscript{55}

Disarmament bodies such as the Intermediate-Range Nuclear Forces Treaty (INF) investigative process also provide key examples of internal accountability frameworks. The INF Special Verification Commission serves as a forum through which state parties can resolve concerns and questions regarding compliance and treaty implementation.\textsuperscript{56} Member states can call meetings of the Special Verification Commission to voice complaints about state party compliance and to try and reach agreement on inspection procedures. The United States and Soviet Union agreed that either country could call a Special Verification Commission meeting to resolve issues of compliance and discuss new measures needed to improve the treaty’s effectiveness.\textsuperscript{57}

Adopting of Internal Accountability

Our research illustrates the importance that internal accountability has in creating a credible organization. Thus, it is important that the proposed organization develop its own internal


\textsuperscript{54} Ibid.

\textsuperscript{55} “Speakers in Security Council Call for Unified, Global Counter-Terrorism Effort, Following Briefings by Chairs of Committees Set Up to Spearhead Fight,” United Nations, May 11, 2010.


\textsuperscript{57} Ibid.
framework for both independent review and peer-reviewed compliance. Doing so will help to strengthen the attribution organization’s external credibility and build trust in the private sector.

As such, the proposed organization should have an independent review body like that of the United Nations Office of the Ombudsperson. Parties who feel they have been wrongfully attributed for a nation state cyberattack could then submit a formal complaint to the organization’s independent review body. The review body will then analyze the investigation process of the disputed attribution to ensure neutrality and evidentiary standards were upheld. They will then publicly submit their report on the investigation with their conclusion on the attribution’s legitimacy. This body will provide an important check on the main investigative team.

Inclusion of Technical and Geopolitical Experts

Private sector and academic expertise is essential to the proposed organization because the credibility of these experts stems from their professional background and reputation—and neutrality. Expertise in both technical forensic analysis and geopolitics allows organizations to ensure that findings will be perceived as legitimate. Two examples from our research stand out in this respect—the Cheonan investigation and the IAEA.

Expert Inclusion Models: The Cheonan Investigation and the IAEA

Despite its lack of transparency, the Cheonan investigation is a good example of incorporating technical experts into the attribution process. The Cheonan sinking investigation is a key case study for combining professional expertise and government authority for reaching attribution judgments. As outlined above, in 2010, the South Korean warship Cheonan sank near North Korea, killing 46 servicemen. The incident heightened tensions between the Koreas even though the North Korean government denied culpability. The United Nations Security Council publicly condemned the attack without identifying the perpetrator. With Chinese, Russian, and US engagement growing in the region, this incident had ramifications beyond the peninsula.
To maintain regional stability, and mitigate against further escalation, South Korea launched a multinational team comprised of experts to determine the cause of Cheonan’s sinking. The group was composed of experts organized into four teams: scientific investigation, explosive analysis, ship structure management and intelligence analysis. Their final report, released to the public in May 2010, determined with a “high possibility” that North Korea was responsible for the attack. The Joint Investigation Group utilized an international body of experts to attribute the attack. The measures the Joint Investigation Organization took, to include individuals with relevant expertise and diverse geographical backgrounds, bolstered the efficiency to determine the responsible adversary in the Cheonan attack.

Another example of a way to incorporate peer review into investigations is the International Atomic Energy Agency’s (IAEA) model. The IAEA clearly outlines the components of a nuclear facility inspection so the public can have confidence that all variables are accounted for in the process. By outlining these steps, the experts establish transparent procedural norms. Creating these procedural norms is critical in legitimizing the IAEA’s findings.

Adopting Expert Inclusion in Investigations

Ultimately, credibility is the goal of the proposed organization’s attribution investigations. Like the Cheonan investigation, the proposed organization could adopt the use of independent experts from diverse geographical backgrounds, into its structure, while avoiding the Cheonan investigation’s transparency missteps. In addition, the IAEA’s transparency and inclusion of experts offers a pathway to legitimacy.

Put into practice, the proposed organization would draw upon a panel of independent cyber experts to conduct the investigation and attribution of cyberattacks. The experts responsible

for forensic analysis would represent diverse geographic representations among global private sector information security firms.

The details of the methodologies and findings from the experts’ attribution process would to be released to hold their actions accountable. Releasing such procedural information will create transparency because the international community will be able to review potential flaws in the attribution process. Additionally, publicly disclosing the attribution processes encourages the experts to transparently conduct their investigations. Clearly communicating the experts’ operations can leave the public more confident in findings.

Private Sector Membership

In addition to the above best practices, any attribution organization meant to tackle state-sponsored cyberattack will be under a high level of scrutiny, making the appearance of neutrality particularly important. While many of the attribution organizations and processes we examined involve governments in attributing responsibility, in the case of this organization it will be imperative to remain independent from perceived nation state influence. Therefore, the proposed organization must be made up of private sector actors—but could include experts drawn from other sectors. The Sony Hack Investigation and the Egmont Group offer support for the need to separate the organization from governments.

Private Sector Membership Models: The Sony Hack Investigation and the Egmont Group

The proposed organization will not include any public sector or governmental bodies. Incorporation of governments into the proposed organization would undermine the organization because government involvement brings lack of transparency and issues of credibility.

Because governments’ primary responsibility is to protect individual nation state security, they are often unwilling to share information and frequently operate without transparency—particularly security agencies. The Sony Hack Investigation highlights the independent and
exclusive nature of the government. The FBI investigated the attack for reasons of national security, while at the same time Sony hired FireEye, an American private cybersecurity firm, to investigate. Although it would have facilitated a more robust investigation, there is no evidence of collaboration between the two entities. In addition, the FBI did not release any detailed information of its investigation or its attribution report. The only release of information was a vague one-page statement indicating North Korea as the culprit. As a result, the expert community viewed the FBI’s findings with skepticism, something that continues to this day.

Because governments do not operate in a transparent manner, they lack the credibility that third parties have and that is needed to run an attribution organization. In many of our case studies, it is apparent that a third party is brought in to either attribute attacks or to provide the tools to attribute those attacks. An example of this is the Egmont Group of Financial Intelligence Units. Its mission is to combat money laundering and terrorism financing operations around the globe. To facilitate effective attribution, the Egmont Group follows a set of procedural norms set out by the Financial Action Task Force, a non-governmental body specializing in creating and updating standards for the fight against money laundering and terrorism financing. The Egmont Group uses procedural norms to train their intelligence units and has accountability groups that track whether these procedural norms are followed.

Furthermore, the standards that the Egmont Group follow are based on multiple United Nations conventions outlining the specific methods in countering monetary criminal activity. Thus, creating distance between those that set up norms and the attributors who use those norms, the Egmont Group, portrays legitimacy and neutrality. In the same way, having an independent group of private sector organizations attributing another level of actors (nation states), consequently provides a level of distance between those who attribute fault, and those who are potentially committing the crime itself.

Adopting Private Sector Membership

Our research, combined with the distinct challenges inherent in a cybersecurity attribution organization, indicates the need for the proposed organization to be a private sector run organization. The need for private sector leadership is because market pressures will ensure company neutrality and hard work. Private sector entities also have access to valuable information for attributing cyberattack. Finally, they have the advantage of speed and flexibility.

Market pressure will ensure that companies work hard to attribute cyberattack—and market pressures will also help to make sure companies remain neutral in attribution. Companies have a growing stake in their own security as the frequency and cost of cyberattacks increase. An expected $3 trillion in costs by 2020 will be attributed to cyber crime. Therefore, private corporations are increasingly concerned about their own security and protecting shareholder value. Joining the proposed organization provides an avenue to bolster protection.

Additionally, private sector members have a wide swath of cyberattack information and technical forensics within their network systems. Sharing this information is essential to make convincing attribution judgements. Drawing on the example of the Egmont Group, we see that private sector information is instrumental in making attribution judgements for money laundering and terrorism financing. The Financial Action Task Force Recommendations mentioned earlier specifically outlines the list of bodies from which Financial Intelligence Units should receive transactional information. The Unit utilizes both cash-transaction reports and suspicious-transaction reports to help make criminal attribution judgement. The bodies that must submit these reports to Financial Intelligence Units include banks, securities dealers, insurers, casinos, and even lawyers and accountants. This diverse array of reporting entities provides Financial Intelligence Units with a comprehensive database of pertinent information

---

that can be analyzed and then transmitted to law-enforcement or prosecutorial entities as needed. The proposed organization, likewise, should have private sector firms from a wide array of industries contribute to a singular source of nation state cyberattack information that can be analyzed thoroughly by industry experts and disseminated in the most appropriate fashion.

Finally, as opposed to government bodies, private sector companies have the advantage of speed and flexibility in sharing information and supporting attribution judgements because they are not impeded by dissimilar jurisdictions present in multinational governments. They would be able to relatively easily provide information to the umbrella organization’s utilization of SecureDrop, an open source software platform for anonymous communication channels.

Potential Membership
Private sector firms that would be interested in joining the proposed organization would include large multinationals from around the world and from myriad of industries. The proposed organization might include companies from the banking, manufacturing, technology, and retails sectors, such as Goldman Sachs, Samsung, Sberbank, Sinopec, ThyssenKrupp, or Zara. Many of the member firms will be companies that have already suffered a major cyberattack, while others will have only experienced minor information security breaches. Still others will want to join to better understand and prevent future cyber threats. Whatever the motives of these firms for joining the proposed organization, the trace evidence held by these companies is invaluable to hold in repositories for further attribution in the future.

Membership would also extend to companies in the IT or cybersecurity industry. Companies in these respective industries will have data from clients they have served. However, only raw data, not analyses, will be shared from these security firms. We discuss the potential challenge of cybersecurity firms sharing data in the Private Sector Cooperation section of our report. The key here is to develop a strong base of needed information sharing from both companies that

---

have experienced cybersecurity breaches, as well as the companies that help patch those cybersecurity breaches.

In focusing membership on private sector firms, we do not propose a complete denial of government involvement. In fact, it will be important to have governments’ support and input. The proposed organization includes a plan to gain governments’ own attribution judgements in a confidential manner that retain their anonymity; this section will be further elaborated in the Sensitive and Confidential Cyber Incident Information section. By having top-notch experts analyze both private sector cyberattack information and public sector information, the proposed organization will make a great leap in bolstering cyber defense around the globe while reducing costs to private sector firms and public sector governments.
The Design of the Proposed Organization

The proposed organization is divided into five main bodies and made up of private sector member companies: (1) the Executive Council of Company Representatives, (2) the Expert Investigation Committee, (3) the Expert Review Committee, (4) the Communications Committee, and (5) the Budget Committee.

Executive Council

The highest-level decision-making body is the Executive Council, composed of representatives from member companies. The Executive Council votes on which cyberattacks undergo investigation by the organization. The process of selecting cases will also undergo a two-thirds majority vote for approval. Member companies appoint representatives to the Executive Council for four-year terms. Term limits are a formal organizational practice to ensure a rotating cast of industry stakeholders in the Executive Council. Council members unanimously vote to suspend firm membership in the organization. The representatives are also responsible for appointing experts to the Expert Investigation Committee composed of geopolitical and technical experts. Each company representative appoints experts and final decision to approve appointment requires a two-thirds majority vote of the Executive Council. The Review Committee, by contrast, is composed of independent academics and technical experts.

The Executive Council adopts the best practices of equitable geographic representation, organizational transparency, internal accountability, and private sector participation.

Expert Investigation Committee

The Expert Investigation Committee is responsible for investigating major state sponsored cyberattacks passed through the Executive Council. With direct access to the Information Repository, the Expert Investigation Committee operates on an evidentiary framework that evaluates the veracity and validity of information from the repository. Experts can also submit formal requests of information from member firms for gathering technical forensics during their investigation.
The Expert Investigation Committee’s attribution report will develop an evidentiary framework similar to the legal burden of proof. The evidentiary framework will ensure that the Expert Investigation Committee builds an attribution judgment based on inculpatory evidence. Since the proposed organization does not prosecute a defendant for a cyberattack, the Expert Investigation Committee’s legal burden is lower than conventional criminal law. Rather, the onus is on the Expert Investigation Committee to construct a coherent depiction of a nation state’s involvement with a combination of technical and geopolitical evidence. The core responsibility for the Expert Investigation Committee is to determine the nation state’s responsibility and motivation for an attack.

The Expert Investigation Committee adopts the best practices of equitable geographic representation, organizational transparency, internal accountability, inclusion of technical and geopolitical experts, and private sector participation.

**Expert Review Committee**

The Expert Review Committee holds the Expert Investigation Committee accountable for the quality of evidence used in the attribution. The Expert Review Committee is the peer-review process for the proposed organization. The Committee, composed of independent academics and private sector researchers, reviews the Expert Investigation Committee’s attribution report prior the official release. The Committee is based on opt-in participation and is voluntary; the Executive Council of Country Councils can veto specific Expert Review Committee members with two-thirds majority vote. It provides the imprimatur for the proposed organization, indicating broad consensus on the attribution judgment. Above all, the Review Committee is the mechanism that upholds the proposed organization’s commitment to of neutrality and evidentiary standards.
The Expert Review Committee adopts the best practices of equitable geographic representation, organizational transparency, internal accountability, inclusion of technical and geopolitical experts, and private sector participation.

Communications Committee

The Communications Committee is responsible for receiving the final attribution reports from the Expert Review Committee as well as the dissemination of the report to the public. The Communications Committee follows a well-defined framework that maintains accountability to the public and openness. All evidence used in the attribution report will be disclosed to the public. The member companies appoint the Committee’s members, upholding the practice of geographic diverse representation in the organizations staff. Members of the Communications Committee will work closely with the media and insure the media publishes the findings accurately. Like media organizations who retain a general counsel, the Communications Committee will work with lawyers in the event of a legal challenges.

The Communications Committee adopts the best practices of equitable geographic representation, organizational transparency, internal accountability, stakeholder outreach and private sector membership.

Budget Committee

Member companies also appoint representatives of Budget Committee. The Budget Committee’s responsibilities include managing and collecting the budget of the proposed organization. The Budget Committee will disclose any cases where member company’s fail to uphold their monetary contributions. The Budget Committee will present these cases of non-compliance to the Executive Council who will then determinate an appropriate response. The Budget Committee determines individual member company’s contributions.

Appendix 3 summarizes the projected costs of the proposed organization. We break down the costs into six different categories, the Expert Investigation Committee, the Expert Review
Committee, the Communications Committee, the Budget Committee, Outreach and Member Relations, and Infrastructure and Operations costs. The Executive Council will not be paid as their work is minimal, although the reputational benefits are high. The projected total cost of the proposed organization will be nearly $40 million in the first year and an estimated $30 million a year in subsequent years.

The Budget Committee adopts the best practices of equitable geographic representation, organizational transparency, internal accountability, and private sector membership.

Information Flow

Figure 1, included again below, captures the direction of information flow. As the figure illustrates, information arrives at the organization through an information repository. As evidence is collected, an Expert Investigation Committee verifies the veracity and authenticity of the evidence. An Expert Review Committee also examines the evidence and the findings of both groups create the substance of the attribution report. The Expert Review Committee disseminates the attribution report to the Communication Committee. The Communication Committee works with the media to publicize the results of the review.
Figure 1: Organizational Chart
Challenges for the Proposed Organization

As a new international organization, the proposed attribution organization will face serious challenges as it gathers evidence and produces attribution judgements following major cyberattacks. In the following section, we identify seven challenges and draw upon examples from our research to craft solutions to each potential challenge. These major challenges include:

- Earning public trust
- Cooperation among competitors
- Industry compliance with organizational norms
- Legal challenges of information sharing
- Collecting sensitive and confidential cyber incident information
- Methods of information sharing
- Sharing information with China and Russia

Earning Public Trust

One of the central goals of the proposed organization is to publish and widely disseminate attribution judgements in a timely manner. To effectively accomplish its mission of holding cyberattack perpetrators accountable and dissuading them from future attacks, the organization must be credible to the public. Without credibility, the proposed organization’s judgements are easily dismissed and cyber attackers are free to continue undermining global Internet security.

The proposed attribution organization will operate independently from national governments and be composed entirely of members from the private sector. While its non-governmental status and transparent organizational structure signal a degree of political neutrality, the organization must actively work to promote its independence if it is to hold a reputation as a credible attribution body. While earning public trust is a potential challenge to any international organization, let alone a nascent attribution body, we can borrow from the policies of
Greenpeace and the International Atomic Energy Agency (IAEA) to best foster the attribution organization’s political neutrality and earn public confidence.

Maintaining Independent Funding
Greenpeace provides an example of exclusively apolitical, independent funding. Greenpeace does not accept donations from governments, corporations, or political parties, and rejects donations from private entities that its governing body believes could compromise its independence, objectives, and integrity. The independence of Greenpeace funding suggests that Greenpeace is an organization that cannot be bought or quieted; Greenpeace is only interested in furthering its mission of public environmental awareness and engagement.

Greenpeace’s funding model has proven successful and serves as a model that the attribution organization should adopt to encourage public trust in its functions. Although its methods are often controversial, the public largely views Greenpeace as an authority on environmental issues. Subsequently, in its forty years of existence, Greenpeace has grown from ten activists operating in Alaska to an organization with 2.9 million members conducting operations in 55 countries. Additionally, Greenpeace is responsible for impactful environmental campaigns, ranging from initiatives to stop drilling in the Arctic and stopping the flow of toxic waste into the ocean. The attribution organization can overcome challenges to public credibility by making a similar promise to reject political funding, allowing it to focus solely on its neutral cyberattack investigations.

Functioning as a Public Resource
The attribution organization can position itself as a public resource that not only attributes cyberattacks, but provides information about its mission in an easily comprehensible manner. The IAEA is an example of an organization that has gained public trust through its clear, informative communication strategy. In recent years, use of nuclear energy has grown

---

increasingly controversial, and nuclear energy is also highly technical, often too complex for the public to understand, further exacerbating mistrust in its use.\textsuperscript{69} To combat public misconceptions, the IAEA shares complex information surrounding nuclear energy in a coherent manner that is easily understood by the public, in the form of factsheets, podcasts, regular bulletins, and informational booklets.\textsuperscript{70} When the public sees the IAEA as an informational resource whose mission is clear and understandable, the IAEA is fundamentally more credible and able to more effectively govern nuclear technology and safety.

The attribution organization can earn public trust in a similar manner. Like nuclear technology, the mechanics of a major cyberattack are highly complex and abstract to everyday citizens. By engaging the global public in the cybersecurity issues it investigates, the organization can build public trust that will in turn yield credence to its attribution judgements, thus, hopefully contributing to the decline of major state-sponsored cyberattacks over time.

**Cooperation among Competitors**

One of the greatest challenges in developing a private sector blueprint for cyberattack attribution is exploring how the proposed organization could advocate and incentivize private sector companies to commit to a process of information sharing and coordinating common resources with firms that are often their competitors. Most companies aim to prevent cyberattacks through focusing on strengthening their internal networks rather than coordinating with competitors.

Additionally, some companies prefer to absorb losses incurred by security breaches rather than reveal weaknesses in cybersecurity systems—all in the name of protecting reputations and shareholder values. However, focus on internal cybersecurity at the expense of industry information sharing and cooperation is highly impractical, as it is nearly impossible for a


company to identify and patch every cybersecurity vulnerability arising in a single network. Information sharing between companies allows for greater understanding of cybersecurity threats can make every company stronger. Yet despite general acknowledgement of the importance of information sharing and the presence of sector specific information sharing bodies such as Information Sharing and Analysis Centers, considerable room for improvement and greater industry cooperation remains.

To overcome the challenge of private sector cooperation, we propose adopting information sharing practices that incentivize greater industry cooperation. The global collaboration exhibited by the Stuxnet Investigation and the Egmont Group of Financial Intelligence Units offer a model that can be adapted to bolster cyber defense and effectively decrease the costs of defense to all organization members.

Incentivizing Cooperation through Access to Resources
As a group of 152 governmental bodies, the Egmont Group is a successful model of how to incentivize cooperation in a way that leads to international cooperation. The Egmont Group is responsible for analyzing financial information shared by banks and financial institutions with the goal of stopping money laundering and terrorist financing. Governments and financial institutions willingly share this sensitive information with the Egmont Group, and by extension, other countries. Governments must apply to be admitted to the Egmont Group, suggesting that governments want to be part of a system of norms and collaboration.

The Egmont Group incentivizes collaboration and information sharing in three key ways. First, governments applying to the Egmont Group gain access to the Group’s wide variety of training resources and to access financial data from other countries, resources that ultimately strengthen a government’s own financial security. Examples of the Egmont Group’s resources

---

72 Gagnon, 2013.
73 “Financial Intelligence Units (FiUs) - The Egmont Group.”
75 International Monetary Fund and World Bank, 2004.
include yearly plenaries and communiques where members discuss the most pertinent case studies in fighting money laundering across the globe, training sessions on implementing Financial Action Task Force Recommendations, and systems set out for anti-money laundering and thwarting terrorism financing organizations. Egmont Group membership also provides access to the resources of the International Monetary Fund and World Bank, who provide technical assistance to the financial intelligence units of member countries. Governments use this information and assistance to more effectively attribute criminal activity within their own borders. Gaining insight from a network of international bodies is particularly useful due to the transnational nature of many financial crimes.

Second, the Egmont Group incentivizes membership through its clear, centralized communication, fostering efficient exchange of information pertinent to timely attribution judgements. The Egmont Group has four working bodies specifically designated to enhance the quality and quantity of information being shared among Financial Intelligence Units, as well as to enhance the methodologies and standards of communications between governments. The benefits reaped from effective, immediate information exchange allow individual governments to reduce the economic and opportunity cost of conducting their own international investigation.

Lastly, Egmont encourages international cooperation through the reputational benefits it affords its members. Members are incentivized to cooperate due to the operational benefits of joining a large organization that allows member governments to more effectively combat activity condemned by not only international law and conventions, but many domestic laws as well. In the eyes of domestic and international audiences, Egmont membership signals a commitment to financial accountability, bolstering a government’s legitimacy and international standing.

77 International Monetary Fund and World Bank, 2004.
Encouraging Cooperation through Privacy Assurances

The Stuxnet Investigation is another useful model of private sector cooperation, especially among companies that are traditionally competitors. In the wake of the Stuxnet attack, Russian security firm and anti-virus provider Kaspersky Lab and the American company Symantec led an ad-hoc investigation to attribute the source of the attack. Their work was not only to attribute responsibility, but to rebuild consumer confidence in the security of Internet data. In addition to working with Symantec, Kaspersky Lab also worked with other competing security firms such as MacAfee, and collaborated with a range of industry and geopolitical experts to approach the investigation. These competitors worked together to share evidence pertaining to Stuxnet and made mutual assurances to keep each other’s data private, fostering more direct cooperation and disclosure.

In the Stuxnet Investigation, the challenge of convincing competitors to cooperate was solved through instituting a system of information sharing with guaranteed privacy assurances. The proposed attribution organization should similarly institutionalize privacy assurances in a way that fosters investigation and evidence collection while preserving each member companies’ competitive edge. As long as each company agrees upon the type of attack data they will share and makes assurances to keep sensitive data private, each company should be able to reap the benefits that accompany cooperation. By following the Stuxnet example, competitors can cooperate while increasing their ability to attribute major cyberattacks in a timely and efficient manner.

Industry Compliance with Organizational Norms

Another challenge in creating an international private sector attribution organization is obtaining industry compliance. For the attribution organization to complete its objectives, its members must adhere to the proposed organization’s processes and established behavioral

---


80 Gagnon, 2013.
norms. The problem of compliance stems from the unwillingness of private firms to voluntarily disclose sensitive information and vulnerabilities, including their own susceptibility to cyberattack. Companies risk exposing themselves to liability suits, a write-down of share-price, and the disclosure information to competitors.

The issue of compliance, however, is not a new dilemma for international organizations. In the following section, we apply rationalist and constructivist theory to address the compliance question for the proposed organization. In assessing behavioral theory, we attempt to delineate several credible reasons companies engage in compliance, principally, to gain security reward and to avoid reputational punishment. This can only be accomplished, however, if companies trust and validate the behavioral norms and standards they must adhere to.

Rationalist Behavior Theory

Rationalist theory argues that private and state actors will undergo a cost-benefit analysis and then only observe international law if compliance outweighs the disadvantages of non-compliance. However, laws alone do not cause companies, or states, to behave in certain ways. Reputational concern and mutual benefits also influence compliance behavior. For example, following the Operation Aurora attacks, executives at Google believed that it was more important to uphold a positive public image than to adhere to China’s strict Internet regulations. Thus, Google lost billions of dollars of potential revenue after exiting the Chinese markets in exchange for maintaining its reputation. Based on this example, and tied to the same incentives that compel cooperation among competitors, it is likely that companies will see participation in such an attribution organization in their benefit.

Constructivist Theory

One of the many foci of constructivist theory examines the issue of reputation in relation to

---

compliance with an international order. Constructivist theory places a greater weight in identity formation and international society to explain compliance motivations than do rationalist approaches.\textsuperscript{84} The constructivist strand of thinking braids together rationalists’ emphasis on self-interest with socially constructed interests. These constructed interests include recognized norms and values that can compel companies to act a certain way to maintain their reputation. Constructivists ascribe successful compliance with behavioral norms to three factors. The three factors that foster stronger willingness to comply with an organization’s rules are efficiency, self-interest, and trust.\textsuperscript{85} Therefore, an organizational model based on discourse, persuasion, and cooperation, rather than coercion will lead to accordance with an international organization’s rules.\textsuperscript{86}

Using Theory to Understand Compliance

We can use these theories to understand the process by which companies’ pursuit of their best interest will shape behavior. Companies obey powerless rules because they are pulled toward compliance by considerations of legitimacy and if members feel that the organization’s rules are equally applied and fair. Designing the proposed organization so that benefits of membership exceed cost of membership is essential; the benefits of enhanced company security, the promotion of general Internet security, and enhanced company reputation must outweigh the risks of information sharing. Trust is essential in motivating companies to comply with an organization’s behavioral norms and processes. Generating trust lies in an organization's process and design. Certain procedural instruments such as transparency, streamlined data collection, independent verification and expert supervision, and a default to disclosure help to promote and maintain trust, and, thus, compliance with the proposed organization’s norms for member behavior.

\textsuperscript{84} Harold Hongju Koh, “Why Do Nations Obey International Law?,” Yale Faculty Scholarship Press (1997), accessed May 23, 2017, \url{http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2897&context=fss_papers}.

\textsuperscript{85} Koh, 1997.

Legal Challenges of Information Sharing

A coordinated effort among private sector actors will require sharing sensitive access to cyber incident information, raising questions about the legality of cross-border information flows. In order to produce accurate attribution judgements, the proposed organization’s information repository is likely to include sensitive information such as controlled unclassified information and personally identifiable information. Practically speaking, a forensic analyst is certain to confront personally identifiable information when investigating a company’s computer, or review emails suspected of phishing attacks,87 giving rise to potential risks of violation of privacy and confidentiality. Disclosure of such sensitive data may violate fiat laws, regulation, and privacy contracts. In addition, it may run up against international agreements—for example, the UN International Covenant on Civil and Political Rights (ICCPR) outlines privacy as an international human right,88 while Article 8 of the European Convention on Human Rights cites privacy rights as a reason to restrict data sharing.89

Although privacy laws may complicate the process of sharing information with the proposed attribution organization, we believe that reconciling this obstacle is not only possible, but the lynchpin for ensuring that organizational membership is diverse and sustainable. We draw upon the example provided by the Financial Industry Regulatory Authority (FINRA) as a solution to legal obstacles to information sharing.

Automating Data Analysis

FINRA is an excellent example of an organization that automates the collection and processing of data in adherence with major privacy laws. FINRA is a private, self-regulatory organization monitoring the United States equity market.90 In this position, it collects information on market

---

prices, equity trading, and other key variables in a centralized database.\textsuperscript{91} While this data is sensitive and ripe for a security breach, FINRA’s database uses an automated program to process daily transactions and detect financial fraud, such as market manipulation, insider trading, and compliance breaches.\textsuperscript{92} FINRA’s automatized data analysis provides clear parameters to data collection while developing norms that maintain a company's legal obligations towards information sharing. By delineating a procedure for communication and evidence gathering, FINRA is a model that handles information sharing in a manner consistent with the privacy and security of personal data.\textsuperscript{93}

The proposed attribution organization can integrate FINRA’s automated information sharing processes into its function, helping to ensure compliance with different privacy laws. First, the automation of data analysis, sorting, and extraction will remove the liability of having humans sort through sensitive information.\textsuperscript{94} Privacy will be further protected by establishing formal norms and procedures for the organization’s gathering, sharing, and preserving evidence.\textsuperscript{95}

Defining how, when, and what information companies can share will be the principal measure to formalize secure information sharing capabilities. For example, following a major cyberattack, digital evidence such as file cases, network port numbers, and registry key values are free of personally identifiable information.\textsuperscript{96} As long as member organizations agree to restrict the collection of evidence to only pertinent data surrounding an attack and similarly agree to the automatization of data analysis, privacy laws can be effectively respected without hindering the attribution process.

Collecting Sensitive and Confidential Cyber Incident Information

Collecting and publishing sensitive information from confidential sources is a major challenge
for the proposed organization. While the organization will foster regular communication channels between members and set clear parameters for information sharing, sometimes evidence pertaining to a cyberattack cannot be obtained by organization members alone. At times, the organization will rely on information from the public to complete its attribution judgements. At other times, the organization may need information that only government agencies can provide.

SecureDrop: A Tool for Anonymity and Sensitive Data Collection from the Public

The proposed organization can guarantee anonymity of sources by using a software application called SecureDrop. As illustrated by the Stuxnet Investigation, information surrounding many major cyberattacks often come from anonymous sources whose privacy must be protected. Anonymous sources function as whistleblowers who risk losing their jobs and may face prosecution. Thus, the proposed attribution organization must find a way to protect sources of confidential, sensitive information while simultaneously maintaining a commitment to a transparent investigative process. Solely relying on classified information could undermine the proposed organization’s legitimacy and commitment to openness, while omitting information from whistleblowers to protect their information would result in incomplete evidence collection and a less-credible attribution judgement. In contrast, when an attribution judgement uses both openly available evidence as well as evidence provided from sensitive sources, a judgement is far more credible and authoritative.

Journalists have long depended on anonymous sources in their work. The Stuxnet Investigation is a case in point. The Washington Post relied upon an anonymous government whistleblower to validate the private sector’s attribution report. With the input of this anonymous whistleblower, the Washington Post helped bolster the credibility of the Stuxnet Investigation’s attribution of the attack to the United States and Israel.97

SecureDrop is software platform is widely used by newspaper organizations that allows

whistleblowers to confidentially share information and communicate with journalists. SecureDrop is integrated into TOR, fully encrypts communications, cannot be accessed by anyone outside the news organization that owns it, minimizes the metadata trail between journalists and sources, and does not track IP addresses. The code for SecureDrop is open source and available to independent oversight. Additionally, SecureDrop is audited by the Freedom of the Press Foundation, a non-profit free speech advocacy group to guarantee its security. SecureDrop is free and internationally accessible, making it a realistic tool for our proposed attribution organization, which will likely be gathering evidence from many countries at one time.

Tearlines: A Mechanism for Receiving Government Information

It is likely that the proposed organization will need to receive classified government information, making a mechanism to ensure the information is secure necessary. A potentially useful mechanism is “tearlines.” Government intelligence agencies use tearlines to share classified information to parties without disclosing the most sensitive information.

For example, the Intelligence Community Directive 209 states that tearlines are, “written for the broadest possible readership in accordance with established information sharing policies, and requirements in law and policy to protect intelligence sources and methods.” Essentially, tearlines help US intelligence agencies disclose, when possible, limited classified information to parties for an investigation, “including by providing [information] to non-Federal entities.”

The use of tearlines is not limited to the US. Tearlines were used by the Pakistan Inter-services Intelligence (ISI) to share classified intelligence with India for the 2008 Mumbai terror attack

---

99 Ball, 2014.
investigation. In regard to a cyberattack attribution case, if the proposed organization requires classified government intelligence, tearlines may be the answer. While there is a possibility the information desired to piece together a cyberattack attribution is the sensitive information above the tearline, tearlines provide a mechanism from which to begin secure information sharing between governments and the proposed organization. Having a mechanism in place to keep a channel open for the government to share classified information can serve as a useful starting point.

Methods of Information Sharing

Once evidence is collected, the organization must find a way to securely exchange information relating to its attribution judgement. There are four common methods of disseminating findings. First, information sharing can be regulated with a formalized agreement, where parties agree what information will be exchanged, how it will be used, and how it will be kept confidential. Second, security clearance-based information sharing practices involve protected channels of communication between intelligence sources—but is fundamentally narrower in scope than a formalized information sharing agreement. Third, organizations can use a trust–based model of communication that lacks formal agreement and is used by a closed group of individuals—usually cybersecurity professionals from different companies—who share information with one another when they see security issues of common concern. Finally, an ad-hoc model of exchange occurs in response to a cyberattack and establishes temporary channels of communication pertaining specifically to a particular attack. It is not uncommon for an ad-hoc model to lay the groundwork for a more formalized method of information sharing in the future.

105 Ibid.
106 Ibid.
107 Ibid.
108 Ibid.
In our research, we found that international organizations tended to use a formalized model of information sharing, while investigative processes tended to use an ad-hoc model. In this section, we propose that the attribution organization adopt an ad-hoc model since it is most inclusive and effective at reducing barriers to information sharing among private actors. In this recommendation, we draw upon the example of the Mumbai Terrorist Attack Investigation’s ad-hoc information sharing structure as an example to follow in the immediate future. However, further down the road, when the attribution organization is more established, a more formalized model of communication, such as the one embodied by the NATO CCD COE, may be of use.

Adopting an Ad-Hoc Method of Exchange

The Mumbai Terrorist Attack investigation is a strong example of ad-hoc information sharing that can be easily adopted by the attribution organization. The 2008 Mumbai attacks have many parallels with the type of state-sponsored cyberattacks the organization will investigate. The Mumbai attacks were geopolitically motivated¹⁰⁹ and originated in Pakistan with the perpetrators having close ties to Pakistani intelligence.¹¹⁰ Because of the close ties to Pakistani Intelligence, the attack is similar to the way a nation state might perpetrate a major cyberattack for geopolitical reasons.

The Mumbai investigation was led by the Indian government and aided by intelligence from the US and UK, culminating in the presentation of an attribution judgement to the Pakistani government. Once the attack took place, an ad-hoc model of information sharing was immediately employed: intelligence units from the US, UK, and India began rapidly sharing evidence with one another. Timely and open information sharing helped India produce an effective attribution judgement, identifying individuals responsible for the attack.

The Mumbai communication model is an example that would be the most immediately applicable to a nascent attribution organization. Following this model, when a cyberattack occurs, all the relevant stakeholders could easily convene to share information pertaining to the specific attack and produce an attribution judgement. Since each major cyberattack is unique in some form or another and involves different victims and perpetrators, not all the members of the attribution organization would necessarily be involved in each investigation. An ad-hoc model is flexible, allowing for the exclusion and inclusion of relevant parties depending on the nature of the attack.

Toward a Formalized Method of Exchange

While ad-hoc methods of information exchange are flexible and useful as the proposed attribution organization begins its operations, establishing a formalized method of exchange would be advisable once trust is fully established between organization members and the public and a diverse set of companies become organization members. A more formalized channel of information sharing will foster greater efficiency, since the centralization of resources will enable faster investigation.

The NATO CCD COE serves as an example of formalized information sharing that can be readily applied to the proposed attribution organization. The CCD COE’s method of information sharing is said to be formalized because inclusion requires membership involving financial contributions to the CCD COE. Because of an established system of trust and confidence, CCD COE members can discuss more than can be covered in an ad-hoc method of exchange. CCD COE members share all information pertaining to cybersecurity with one another, not just information pertaining to one cyberattack. In this sense, CCD COE members have a fuller shared understanding of the global cybersecurity landscape and can plan more effectively and efficiently for investigations. For example, the CCD COE has produced the Tallinn Manual, holds the annual CyCon conference, and conducts cyberattack and cyber defense exercises. These

---


activities strengthen the cybersecurity of CCD COE members. If the attribution organization can formalize its method of information sharing, it has the potential to expand its investigative capacities and fundamentally enhance global Internet security.

Sharing Information with China and Russia

Not only is there no universal approach to information sharing, but further complicating prospects of global cooperation within the attribution organization are existing geopolitical rivalries and differing approaches to Internet governance. While many major technology companies are located within the US, China and Russia are the other two major actors in international cyberspace. Each has barriers to sharing information and, along with the US, each is a potential source of state-sponsored cyberattacks.

The Chinese government tends to maintain stricter control over private sector information sharing than countries such as the United States. China’s 2016 Cybersecurity Law constrains the ability of the private sector to share information deemed “state secret,” while leaving the definition of “state secret” ambiguous. The ambiguity then makes companies hesitant to share data with each other, let alone their international counterparts.\(^\text{113}\) Furthermore, Chinese technology companies tend to adhere to the government’s policies because they are financially rewarded for compliance with the state.\(^\text{114}\) This dynamic serves as a disincentive for Chinese companies to cooperate with entities outside the country.

Similar obstacles to international private sector cooperation exist in Russia. Russian companies have demonstrated their desire to share information with their global counterparts on several occasions, but tumultuous domestic and international politics sometimes scare companies into silence. For example, the Russian-based security company Kaspersky Lab demonstrated its willingness to cooperate and share information during the Stuxnet Investigation. However,


Russian authorities arrested Kaspersky’s leading investigator on treason charges in late 2016, allegedly for aiding the FBI’s investigation of Russian involvement in the 2016 United States presidential elections.\textsuperscript{115} Around the same time, the United States government restricted Kaspersky Lab’s access to American market due to its suspected collaboration with Russia’s security services.\textsuperscript{116} Thus, Kaspersky Lab has scaled back significantly on its cooperation with non-Russian partners.\textsuperscript{117}

Companies in both China and Russia operate in a delicate political environment. On one hand, these companies recognize the importance of international information sharing. On the other hand, they must balance obedience to domestic law or face heavy political and financial penalties. Additionally, when Chinese and Russia companies collaborate on an international level, they are often met with suspicion from the other countries.

However, different approaches to information sharing need not be a barrier to greater international cooperation and the production of timely, effective attribution judgements. We can encourage greater information sharing and global cooperation with Russia and China through joint security ventures in other parts of the world and through the creation of technology outreach programs.

Engaging the Private Sector

The key to gaining Russian and Chinese private sector cooperation is to build on the common ground shared by all technology companies. For example, while Kaspersky Lab may be viewed controversially in the United States, Kaspersky Lab also completes projects that many American companies would also view as important and non-controversial. For example, Kaspersky Lab shares intelligence with Interpol as they investigate cyberattacks in Southeast Asia.\textsuperscript{118} Chinese


\textsuperscript{117} Flintoff, 2015.

security companies also cooperate with other countries.\textsuperscript{119} It appears that if information technology security companies in Russia and China stay out of their national governments’ business and comply with government policies on information sharing, these companies can still participate in international cyberattack investigations elsewhere in the world. Thus, information technology companies in Russia and China can still become important members of the proposed attribution organization while adhering to their national policies.

In addition, the attribution organization can engage with the private sector in China and Russia through a series of outreach and training programs. Such training programs can include cross-border programs on combating state-sponsored cyberattacks and creating joint technology ventures to build trust between companies operating with different political perspectives.\textsuperscript{120} Programs like these create ground for greater international cooperation and information sharing in the future.

\textsuperscript{119} Ians, 2017.

Conclusion

The advantages of formalizing the investigation of cyberattack attribution into an international organization are apparent. Through centralized information sharing practices and private sector cooperation, key processes of attributing a major cyberattack, such as evidence collection and analysis, can be done better and faster. A network of coordinated private sector actors can quickly collect of a multitude of technical forensics, witness statements, and critical geopolitical information; on its own, a single piece of evidence is insubstantial, but an array of evidence creates a clearer picture, often answering the question of attribution following a major cyberattack.

The proposed organization can build public confidence in its attribution judgments through inclusion and transparency. Ensuring that the processes of collecting evidence and its analysis is disclosed to the public reinforces the credibility of the attribution report. Similar procedural norms that encourage peer-review will further enhance organizational accountability, while transparent, non-governmental membership fosters autonomy from geopolitical influence. Additionally, the proposed organization will benefit from a diversity of perspectives by including private sector companies from across the globe.

The need for greater private sector collaboration in cyberspace is clear. As the likelihood of attribution increases, future cyberattacks will be deterred and perpetrators will be identified. An international organization tasked with attribution is clearly the next step in fostering greater global Internet security, and the private sector has the expertise and resources to see it through.
Appendix 1: International Organizations

Each of the following intergovernmental or nonprofit organizations has an established system of authority and standards for compliance. We have identified both private and public stakeholders involved with each organization and analyzed each organization’s objectives, governance, attributive powers, and budget before compiling a set of best practices from each party.

We examined the following 14 organizations:

- Amnesty International
- Citizen Lab
- Egmont Group of Financial Intelligence Units
- European Financial Coalition Against Child Pornography
- Financial Industry Regulatory Authority
- Greenpeace
- International Atomic Energy Agency
- International Civil Aviation Organization
- International Labor Organization
- NATO Cooperative Cyber Defense Center of Excellence
- Organization for the Prohibition of Chemical Weapons
- United Nations Al-Qaida Sanctions Committee
- United Nations Sanctions Committee on North Korea
- World Trade Organization’s GATT Article XX.
### Actors

<table>
<thead>
<tr>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Researchers, journalists, non-governmental organizations (NGOs)</td>
<td></td>
</tr>
</tbody>
</table>

### Actions

- Investigates human rights abuses, lobbies governments, and promotes outreach campaigns[^121]

### Authority

- Reputational

### Structure

- An international secretariat body and international board provide general leadership
- Regional sections exist in 70 countries around the world[^122]

### Norms

- Statute of Amnesty International (2005)

### Attribution

- Publicly publishes research on human rights violations
- Organization abides by an open information policy

### Budget and Funding Source(s)

- $250 million (2016)
- Funded by independent donations[^123]

### Best Practices

- Prominent regional divisions foster greater international cooperation
- High level of transparency


## Citizen Lab

<table>
<thead>
<tr>
<th><strong>Actors</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- University of Toronto-based interdisciplinary research lab</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

| **Actions** | | |
| - Engages on the core issues of Internet openness and security from a human rights perspective<sup>124</sup> | - Reports are published publicly, sometimes with media<sup>125</sup> |

| **Authority** | | |
| - Reputational<sup>126</sup> | |

| **Structure** | | |
| - A global research network<sup>127</sup> | |

| **Norms** | | |
| - Procedural transparency<sup>128</sup> | - Diverse geographic representation<sup>129</sup> |
| - Academic peer-review<sup>130</sup> | - Open source sharing of information and technical tools<sup>131</sup> |

| **Attribution** | | |
| - Makes all findings public, often directly implicating actors<sup>132</sup> | |

| **Budget and Funding Source(s)** | | |
| - Private foundations, institutes, and organizations<sup>133</sup> | |

| **Best Practices** | | |
| - Mixed method approach to investigation and analysis; combines technical and geopolitical expertise | |
| - Geographic diversity, engages in capacity building with members from the Global South | |
| - Stakeholder outreach via organizing and participating in global conferences | |
| - Autonomy from government and commercial interests | |

---


<sup>127</sup> Ibid.


<sup>131</sup> Elash, 2016.

<sup>132</sup> Ibid.

<sup>133</sup> “About the Citizen Lab.”
### Actors

<table>
<thead>
<tr>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial institutions and non-financial institutions</td>
<td>Financial Intelligence Units (FIU)</td>
</tr>
</tbody>
</table>

### Actions

- Submits cash-transaction and suspicious activity reports to the appropriate FIUs<sup>134</sup>
- Different types of FIUs have different objectives
- Some FIUs notify proper agencies to enforce laws, freezing and blocking suspicious transactions and accounts, and arrest suspects<sup>135</sup>

### Authority

- Corporate Executives and Boards of Directors
- Domestic law
- United Nations (UN) Conventions<sup>136</sup>

### Structure

- Varies by institution
- Each FIU has its own complex structure, dense network of internal bodies, and process-specific groups<sup>137</sup>

### Norms

- Managerial discretion
- Local and/or national law
- 2003 Financial Action Task Force (FATF) recommendations based on Vienna and Palermo Conventions<sup>138</sup>
- FATF recommendations<sup>139</sup>

### Attribution

- No attributive properties; works solely as an information-gathering organization
- Name organizations that fail to uphold reporting standards and laws<sup>140</sup>
- Attribution information is shared between FIUs through communiques, plenary meetings, and trainings<sup>141</sup>

### Budget and Funding Source(s)

- Budgets vary from institution to institution
- Budgets vary from nation to nation
- Funds for each institution are acquired through debt and equity
- Funding provided by national governments
- United States FIU (FinCEN) has proposed budget of approximately $155M in 2017<sup>142</sup>

### Best Practices

- Suspicious Activity Reports function as preventative measures that can also provide information needed to launch criminal investigations
- Process Improvement Groups promote information exchange and adherence to financial standards created by the Egmont Group
- Heavy emphasis on communication and training mechanisms ensure cooperation and cohesion

---


<sup>135</sup> Ibid.


<sup>138</sup> International Monetary Fund, and World Bank, 2004.


<sup>142</sup> International Monetary Fund, and World Bank, 2004.
## European Financial Coalition Against Child Pornography (EFCACP)

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Banks, payment companies, Internet service providers</td>
<td>- Europol, European Union (EU)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Co-operates with the EFCACP to design and launch initiatives to stop the sexual exploitation of children online</td>
<td>- Fights sexual exploitation of children online by disrupting the economics of the illegal industry</td>
</tr>
<tr>
<td></td>
<td>- Works to prevent the transferring of funds for child pornography through credit cards and other online payment methods</td>
<td>- Promotes awareness, cross-sector training sessions, and policy research and promotion&lt;sup&gt;144&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>- ISPs work to implement a better system for detecting and blocking pornographic content&lt;sup&gt;143&lt;/sup&gt;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authority</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Reputational</td>
<td>- EU</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Structure</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Partnerships are established on a voluntary basis</td>
<td>- Bureaucratic; one of many regional branches of the Financial Coalition Against Child Pornography</td>
</tr>
<tr>
<td></td>
<td>- Representatives from private industry sit on the Steering Committee&lt;sup&gt;145&lt;/sup&gt;</td>
<td>- The EFCACP is chaired by Europol and led by a Steering Committee Functions as a branch of the European Cyber Centre at Europol</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Norms</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- UN Convention on the Rights of the Child</td>
<td>- UN Convention on the Rights of the Child</td>
</tr>
<tr>
<td></td>
<td>- NGO/Industry best practices</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribution</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- No attributive properties</td>
<td>- No attributive properties, but shares information with other EU bodies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Budget and Funding Source(s)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Part of Europol’s $114.6 million budget (2017)</td>
<td>- Funding provided by EU member states&lt;sup&gt;146&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Best Practices</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Wide range of private actors from multiple fields have a seat at the table and are involved in the organization’s structure and agenda</td>
<td>- Prominent regional divisions foster greater international cooperation</td>
</tr>
<tr>
<td></td>
<td>- The private sector is directly responsible for carrying out initiatives to stop any financial gain related to child sexual exploitation</td>
<td></td>
</tr>
</tbody>
</table>

---


### The Financial Industry Regulatory Authority (FINRA)

<table>
<thead>
<tr>
<th><strong>Actors</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Self-regulating private corporation</td>
<td>- Securities Exchange Council (SEC), Justice Department, and the Federal Bureau of Investigation (FBI)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Actions</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Monitors US equities, shares information with authorities</td>
<td>- Use FINRA's information to build evidence for the prosecution of securities fraud</td>
</tr>
<tr>
<td></td>
<td>- Protects investors by upholding the integrity of US financial market, and levies fines against brokers</td>
<td>- The Securities and Exchange Act; SEC’s extraterritorial exercise of its jurisdiction</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Authority</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Performs regulatory oversight of securities firms selling to public investors through contracts with stock exchanges</td>
<td>- Bureaucratic agencies within the federal government</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Structure</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- 3,400 employees based in Washington, D.C. and New York City with 20 regional offices</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Norms</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Complies with the Federal Reserve and laws regulating data and information privacy</td>
<td>- Press briefings, disclosure, laws regulating evidence collection and prosecution</td>
</tr>
<tr>
<td></td>
<td>- Uses an arbitration forum</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Board members are publicly elected</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Attribution</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Discloses information publicly in reports and with law enforcement</td>
<td>- Yes, and prosecution</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Budget and Funding Source(s)</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- $878.6 million (2012)</td>
<td>- Budget is provided by the US government</td>
</tr>
<tr>
<td></td>
<td>- Funded by the businesses it regulates</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Best Practices</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Public disclosure</td>
<td>- Strong norms and laws guide investigations</td>
</tr>
<tr>
<td></td>
<td>- Use of technology to detect fraud, centralized database</td>
<td>- Public disclosure</td>
</tr>
<tr>
<td></td>
<td>- Collaboration with authorities</td>
<td>- Public-private cooperation</td>
</tr>
</tbody>
</table>

---


148 Ibid., 8

149 Ibid., 72.


154 Ibid., 8

<table>
<thead>
<tr>
<th><strong>Actors</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>Members and volunteers</td>
<td></td>
</tr>
</tbody>
</table>

| **Actions** | - Research and lobbying on cases of environmental destruction |

| **Authority** | - Reputational  
|              | - Consultative status with UN Economic and Social Council |

| **Structure** | - 26 regional offices report to the headquarters office of Greenpeace International in Amsterdam  
|              | - Regional offices deal with issues at a local level, while the headquarters take on issues that have broader global implications\(^{156}\) |

| **Norms** | - Responsibility, nonviolence, independence and neutrality, as listed in Greenpeace's core values \(^{157}\) |

| **Attribution** | - Operates a "fleet" consisting of four ships, hot air balloons, inflatables, and remote sensing tactics to surveil the areas they are inspecting  
|                | - Inspections are carried out by their volunteers and employees \(^{158}\) |

| **Budget and Funding Source(s)** | - $349.8 million (2015), collected from donations of 2.9 million members \(^{159}\) |

| **Best Practices** | - Independence from public sector  
|                   | - Strong reputational authority |

<table>
<thead>
<tr>
<th><strong>Actors</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Atomic energy experts and employees</td>
<td>- 168 member states</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Actions</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Set nuclear safety standards</td>
<td>- Comply with Safeguards/Additional Protocol</td>
</tr>
<tr>
<td></td>
<td>- Help member states meet safety standards</td>
<td>- Declare all nuclear facilities and materials, aid other member states ²⁶¹</td>
</tr>
<tr>
<td></td>
<td>- Verify compliance with international safeguards ²⁶⁰</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Authority</strong></th>
<th><strong>UN</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Individual member states report to the Board of Governors, General Conference</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Structure</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- The Secretariat consists of five offices and six departments staffed by experts from the private sector</td>
<td>- National energy agencies, such as the US Nuclear Regulatory Commission and the Department of Energy, work alongside IAEA offices and departments ²⁶²</td>
</tr>
<tr>
<td></td>
<td>- Board of Governors consisting of representatives from 22 member states; each state must be elected by the General Conference</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- The General Conference contains delegates of all 168 member states that meet once a year to approve actions and budgets</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Norms</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Based around the policy of nuclear non-proliferation</td>
<td>- Each state is bound to the Safeguards/Additional Protocol</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Attribution</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Attribute safety violations through materials and facilities inspections ²⁶³</td>
<td>- States can attribute domestic problems by conducting self-evaluation and peer-review inspections before official IAEA inspections</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Budget and Funding Source(s)</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- $391.5 million (2016) ²⁶⁴</td>
<td>- Each member state has its own energy budget</td>
</tr>
<tr>
<td></td>
<td>- Funded by member states and other donations</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Best Practices</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Political neutrality</td>
<td>- Emphasis on cooperation between government agencies</td>
</tr>
<tr>
<td></td>
<td>- Collaboration within the private sector</td>
<td>- Provide a framework for self-assessment</td>
</tr>
<tr>
<td></td>
<td>- Different branches of the organization serve as a form of checks and balances</td>
<td>- Have formal agreements, such as the founding statute and Safeguard, that act as the basis for IAEA operation</td>
</tr>
</tbody>
</table>

### International Civil Aviation Organization (ICAO)

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Airlines, tourism offices, and airplane manufacturers&lt;sup&gt;165&lt;/sup&gt;</td>
<td>- 191 UN member states</td>
</tr>
<tr>
<td>Actions</td>
<td>- Collaborate with UN agencies to further civil aviation’s progress and strategize non-state actor involvement with the ICAO&lt;sup&gt;166&lt;/sup&gt;</td>
<td>- Uses consensus on Standards and Recommended Practices (SARPs) made by Member States to conduct safety and security audits&lt;sup&gt;168&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>- Offer consultation services to ICAO when requested, usually regarding the adoption of new standards and practices&lt;sup&gt;167&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td>Authority</td>
<td>- Reputational</td>
<td>- UN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Chicago Convention on International Civil Aviation</td>
</tr>
<tr>
<td>Structure</td>
<td></td>
<td>- Member states sit on an Assembly to vote on all SARPs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Member states elect a council of 36 states that provide overall direction of organization and elects a president</td>
</tr>
<tr>
<td>Norms</td>
<td>- ICAO SARPs</td>
<td>- Chicago Convention on International Civil Aviation</td>
</tr>
<tr>
<td>Attribution</td>
<td>- No attributive properties; shares reviews with ICAO&lt;sup&gt;169&lt;/sup&gt;</td>
<td>- Publicly shares safety audit results, naming breaching parties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security audits remain internal, and no attribution for security breaches are publicly named&lt;sup&gt;170&lt;/sup&gt;</td>
</tr>
<tr>
<td>Budget and Funding Source(s)</td>
<td></td>
<td>- $221.12 million (for 2017-2019)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Funded by member states and private industry&lt;sup&gt;171&lt;/sup&gt;</td>
</tr>
<tr>
<td>Best Practices</td>
<td>- Collaboration with the public sector</td>
<td>- Keeps updated norms to meet technological advancements&lt;sup&gt;172&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>- Utilization of private sector expertise</td>
<td>- Incorporation of private industries and their specialties</td>
</tr>
</tbody>
</table>


<sup>166</sup> Ibid., 36


<sup>170</sup> Ibid., 40


<table>
<thead>
<tr>
<th><strong>Actors</strong></th>
<th><strong>Private</strong></th>
<th><strong>Public</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- 187 member states</td>
</tr>
<tr>
<td><strong>Actions</strong></td>
<td></td>
<td>- Represents employment and workers, registers complaints, sets global labor standards, and investigates violations of workers’ rights.</td>
</tr>
<tr>
<td><strong>Authority</strong></td>
<td></td>
<td>- UN Charter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ILO Conventions</td>
</tr>
<tr>
<td><strong>Structure</strong></td>
<td></td>
<td>- ILO functions as a “Parliament of Labor,” where a Governing Body oversees the International Labor Conference, where government, employer, and worker delegates from each country debate policy</td>
</tr>
<tr>
<td><strong>Norms</strong></td>
<td></td>
<td>- Routine monitoring, free and open debate, declaration of fundamental principles, equal geographic representation, and a tripartite government structure</td>
</tr>
<tr>
<td><strong>Attribution</strong></td>
<td></td>
<td>- Release findings after a process of evidence collection, standardization, assessment of legal burden, and a review process</td>
</tr>
<tr>
<td><strong>Budget and Funding Source(s)</strong></td>
<td></td>
<td>- $225.7 million (2015)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Funded by contributions from member states and donations</td>
</tr>
<tr>
<td><strong>Best Practices</strong></td>
<td></td>
<td>- An efficient system to launch complaints and establish transparency reports</td>
</tr>
</tbody>
</table>

---


## NATO Cooperative Cyber Defense Center of Excellence (CCDCOE)

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Companies in the defense industry, such as Siemens, Thread \ Systems, Cyber Test Systems, and more</td>
<td>NATO member states and cooperating non-member states</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th></th>
<th>Promote cooperative cyber defense, establish cyberspace norms, and confidence-building measures&lt;sup&gt;179&lt;/sup&gt;</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Authority</th>
<th></th>
<th>NATO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>International steering committee consisting of center’s sponsoring nations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The CCDCOE is not part of NATO’s military command or force structure, and is made up of military, government, and defense industry professionals</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Center consists of researchers, analysts, trainers, educators&lt;sup&gt;180&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Norms</th>
<th></th>
<th>Tallinn Manual&lt;sup&gt;181&lt;/sup&gt;</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Attribution</th>
<th></th>
<th>Attributes cyberattacks in published articles, but is mostly focused on building cyberinfrastructure, and cyberdefense capabilities&lt;sup&gt;182 183&lt;/sup&gt;</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Budget and Funding Source(s)</th>
<th></th>
<th>Funded by NATO and Non-NATO members</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Best Practices</th>
<th></th>
<th>Multinational information sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Promoting collective cyberdefense</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accumulating, creating, and disseminating international cyberexpertise</td>
</tr>
</tbody>
</table>

<sup>180</sup> Structure | CCDCOE,” accessed May 4, 2017, [https://ccdcoe.org/structure-0.html](https://ccdcoe.org/structure-0.html).
<sup>183</sup> Jason Rivera and Forrest Hare, “The Deployment of Attribution Agnostic Cyber defense Constructs and Internally Based Cyber threat Countermeasures,” CCD COE, 6th International Conference on Cyber Conflict, 2014, 100–116.
## Organization for the Prohibition of Chemical Weapons (OPCW)

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Independent scientists and NGOs</td>
<td>192 member countries</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>Overseas outreach and training programs with chemical industry</td>
<td>- Carries out verification measures, facilitates chemical weapons inspections, and negotiates agreements with state parties</td>
</tr>
<tr>
<td>-</td>
<td>Collaborates to review processes of verification and chemical weapons disarmament</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authority</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Reputational</td>
<td>- UN</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Structure</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Independent scientists sit on the Scientific Advisory Board</td>
<td>- Led by a Director-General</td>
<td></td>
</tr>
<tr>
<td>- INGOs like the International Union of Pure and Applied Chemistry provide a consultative and outreach role</td>
<td>- Equitable geographic distribution in decision-making bodies</td>
<td></td>
</tr>
<tr>
<td>- Private companies can sign a Memorandum of Understanding with the OPCW to solidify cooperation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Norms</th>
<th></th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Attribution</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- No public attributive properties; private actors do not release information about ongoing investigations</td>
<td>- No public attributive properties; do not release information about ongoing investigations</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Budget and Funding Source(s)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- $95 Million (2012)</td>
<td>- Funded by member states, whose contribution is calculated based on the UN scale of assessment</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Best Practices</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Involves chemical industry in outreach training programs and norms building</td>
<td>- Equitable geographic distribution among all bodies of the organization</td>
<td></td>
</tr>
<tr>
<td>- Scientists actively participate in advising and facilitating disarmament on a rotational and elected basis</td>
<td>- On-the-ground inspections and fact-finding missions give the OPCW a tangible presence in member countries</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Broad international treaty gives the organization a clear legal mandate and set of duties</td>
<td></td>
</tr>
</tbody>
</table>

---


### United Nations Al-Qaida Sanctions Committee

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Monitoring Team comprised of independent researchers and experts</td>
<td>UN member states</td>
</tr>
</tbody>
</table>

| Actions | - Assists committee and UN member states in identifying and gathering information on sanctioned individuals and monitors cases of state non-compliance with sanction operations | - Imposes a travel ban, freezes assets, and imposes arms embargo sanctions onto individuals or entities believed to be in connection to ISIL or Al-Qaida |

| Authority | - UN | UN |
| Structure | - Independent branch of the Sanctions Committee | - Decision-making done through member state consensus - All members of the UNSC are represented |

| Norms | United Nations Security Council (UNSC) Resolution 1267 | UNSC Resolution 1267 |

| Attribution | - Presents findings to UNSC/UN Sanctions Committee | - Publicly discloses the sanctions list |

| Budget and Funding Source(s) | - Part of Committee budget | - $39.6 million (2015) for all Sanctions Committees - Funded by contributions from UN member states |

| Best Practices | - Cooperate directly with member states in implementation and information-gathering - Conducts independent assessments and ensure compliance and state accountability | - Ombudsperson helps with legal credibility and internal accountability - High level of cooperation with multiple UN and non-UN organizations demonstrates reputational authority and serves as an example of efficacy across sectors and borders |

---


190 Ibid., 55.


## United Nations Sanctions Committee on North Korea

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Panel of Experts composed of professionals from nuclear, weapon of mass destruction, import/export controls, and financial industries[^194]</td>
<td>- UN member states</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th>- Helps the Sanctions Committee gather evidence, analyze information, and assess the implementation of sanctions</th>
<th>- Imposes constraints on diplomats, inspects suspicious cargo, and expands a blacklist of items North Korea is prohibited from importing[^196]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority</td>
<td>- UN, US law</td>
<td>- UN</td>
</tr>
<tr>
<td>Structure</td>
<td>- Panel acts under the direction of the Sanctions Committee</td>
<td>- Centralized bureaucracy with decision-making done through member state consensus[^198]</td>
</tr>
<tr>
<td>- Panelists are appointed by UN Secretary General[^197]</td>
<td>- All members of the UNSC are represented</td>
<td></td>
</tr>
</tbody>
</table>

| Norms | - Purely informational, advisory role with no decision-making capacities[^199] | - A system of routine monitoring, narrow mandate, impromptu meetings, a declaration of fundamental principles[^200] and geographic representation[^201] govern UNSC Resolutions relating to North Korea |

| Attribution | - Publicly publish reports on findings on an annual basis[^202] | - Sanctions list is public, naming specific industries |

<table>
<thead>
<tr>
<th>Budget and Funding Source(s)</th>
<th>- Funded by UN Sanctions Committee, UN member states</th>
<th>- Part of the UN budget for the Security Council and Sanctions Committees[^203]</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Funded by contributions from UN member states</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Best Practices | - Integration of private sector experts into the decisions of a large, inter-governmental body | - Useful model for many countries that agree upon attribution to coordinate and assess fault and compliance |


[^195] Ibid.


[^197] Ibid.


<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Environmental activists</td>
<td>WTO member states</td>
</tr>
<tr>
<td>Actions</td>
<td>Aim to broaden the scope of Article XX&lt;sup&gt;204&lt;/sup&gt;</td>
<td>Promote free trade while protecting and respecting the environment&lt;sup&gt;205&lt;/sup&gt;</td>
</tr>
<tr>
<td>Authority</td>
<td>Reputational</td>
<td>WTO</td>
</tr>
<tr>
<td>Structure</td>
<td></td>
<td>Disputes are mediated through the panel process&lt;sup&gt;206&lt;/sup&gt; - WTO governance is centralized and bureaucratic, with a General Council and committees regulating different aspects of trade</td>
</tr>
<tr>
<td>Norms</td>
<td>Promote environmentally sustainable economic practices</td>
<td>GATT Article XX</td>
</tr>
<tr>
<td>Attribution</td>
<td></td>
<td>Member states can attribute violations to other states&lt;sup&gt;207&lt;/sup&gt;</td>
</tr>
<tr>
<td>Budget and Funding Source(s)</td>
<td></td>
<td>$198 million (2016)&lt;sup&gt;208&lt;/sup&gt; - Funding is provided by contributing Member State trust funds and WTO publications&lt;sup&gt;209&lt;/sup&gt;</td>
</tr>
<tr>
<td>Best Practices</td>
<td>Cooperate directly with member states in implementation and information-gathering - Conducts independent assessments to ensure compliance and state accountability&lt;sup&gt;210&lt;/sup&gt;</td>
<td>Dispute settlement structure</td>
</tr>
</tbody>
</table>

---


<sup>207</sup> Ibid., 69


Appendix 2: Investigative Processes

Each of these investigative processes was formulated and governed in an ad-hoc manner, borrowing authority and structure from a variety of different sources. We have identified both private and public stakeholders involved with each investigative process and analyzed each processes’ objectives, governance, attributive powers, and budget before compiling a set of best practices from each party.

We examined the following nine investigative processes:

- Cheonan Joint Investigation Group
- Democratic National Committee Email Leak Investigation
- Google’s Operation Aurora
- Intermediate-Range Nuclear Force Treaty Investigative Process
- Malaysia Airlines Flight 17 (MH17) Crash Investigation
- Mandiant’s APT1
- Mumbai Terrorist Attack Investigation
- Sony Pictures Hack Investigation
- Stuxnet Investigation
# Cheonan Joint Investigation Group (JIG)

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Media, academia, independent researchers(^{211})</td>
<td>- South Korean Government, technical and forensic experts in the Joint Investigation Group(^{212})</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Test and verify the JIG’s report</td>
<td>- Determine the cause of Cheonan’s sinking and deescalate tensions with North Korea(^{213})</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authority</th>
<th>|</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Credibility of individual organizations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Structure</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- The joint civilian-military team consists of 25 experts from ten domestic professional institutes, 22 military experts, three lawmakers and 24 foreign experts from the US, Australia, the United Kingdom, and Sweden</td>
<td>- State-integrated, non-bureaucratic</td>
</tr>
<tr>
<td></td>
<td>- The JIG was divided into four departments: forensic science, explosive pattern analysis, hull structure, and data analysis(^{214})</td>
<td></td>
</tr>
</tbody>
</table>

| Norms | |
|-------| |
|       | - Peer-review, high-degree of transparency |

<table>
<thead>
<tr>
<th>Attribution</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Evidence analysis and attribution judgment(^{215})</td>
<td>- Published an attribution report detailing evidence collection, evidence standard and analysis, and made final judgement in report(^{216})</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Budget and Funding Source(s)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Funded by South Korean government</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Best Practices</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Decentralized peer-review</td>
<td>- Objective reading of evidence, default to neutrality</td>
</tr>
<tr>
<td></td>
<td>- Accessibility, low-barrier to entry</td>
<td>- Quick investigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Body composed of forensic and technical experts</td>
</tr>
</tbody>
</table>


Democratic National Committee (DNC) Email Leak Investigation

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DNC, Crowdstrike, FireEye</td>
<td>FBI, Central Intelligence Agency (CIA), Department of Homeland Security (DHS), Director of National Intelligence</td>
</tr>
<tr>
<td>Actions</td>
<td>DNC tasked Crowdstrike to investigate and attribute spear phishing and data theft of their campaign(^{217})</td>
<td>FBI initially notified DNC of sophisticated spear phishing(^{219}) and agencies investigated for attribution</td>
</tr>
<tr>
<td></td>
<td>FireEye had an ongoing investigation since 2007(^{218}) and conducted separate attribution investigation</td>
<td></td>
</tr>
<tr>
<td>Authority</td>
<td>Credibility of Crowdstrike as independent organization and FireEye as one of the top four cybersecurity firms(^{220})</td>
<td>US law</td>
</tr>
<tr>
<td>Structure</td>
<td>Ad-hoc individual non-coordinated investigation</td>
<td>Ad-hoc non-integrated investigations except FBI &amp; Dept. Homeland Security</td>
</tr>
<tr>
<td>Norms</td>
<td>Crowdstrike: no peer review, low-degree of transparency</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fire Eye: no peer review, medium-degree of transparency</td>
<td></td>
</tr>
<tr>
<td>Attribution</td>
<td>Crowdstrike did not publish a report of their findings, instead they informed the public of Russian attribution through their website blog(^{221})</td>
<td>FBI &amp; DHS published a report of attribution(^{223}) Director of National Intelligence also produced a report of attribution(^{224})</td>
</tr>
<tr>
<td></td>
<td>FireEye released a report of their ongoing investigation of APT 28 &amp; 29(^{222})</td>
<td>All reports separately attributed Russian involvement in the DNC hacks</td>
</tr>
<tr>
<td>Budget and Funding Source(s)</td>
<td>Provided by DNC</td>
<td>Unknown</td>
</tr>
<tr>
<td>Best Practices</td>
<td>Information sharing</td>
<td>Public release of report</td>
</tr>
<tr>
<td></td>
<td>Expert Analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Report Release</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shorter (than public) investigation time</td>
<td>Cross-verification mechanisms</td>
</tr>
</tbody>
</table>


\(^{219}\) Ibid., 79


## Google’s Operation Aurora

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Google, other tech firms, private security firms, the media[^225]</td>
<td>US intelligence agencies[^226]</td>
</tr>
<tr>
<td>Actions</td>
<td>Investigated attack on Google and the theft of IP and attribution[^227]</td>
<td>Assisted Google as they investigated attacks</td>
</tr>
<tr>
<td>Authority</td>
<td>Reputational</td>
<td>Legal authority within the US and overseas to collect and share data[^228]</td>
</tr>
<tr>
<td>Structure</td>
<td>Independent, non-bureaucratic, state-integrated</td>
<td>Bureaucratic, with limited collaboration with industry[^229]</td>
</tr>
<tr>
<td>Norms</td>
<td>Broke with norms by violating US Computer Fraud and Abuse Act’s criminal provisions[^230]</td>
<td>Confidential information, lack of transparency, governed by the National Security Act of 1947, interagency cooperation</td>
</tr>
<tr>
<td>Attribution</td>
<td>Collected evidence and released findings[^231]</td>
<td>Played a role in evidence collection and did not attribute explicitly but condemned China explicitly[^232]</td>
</tr>
<tr>
<td>Budget and Funding Source(s)</td>
<td>Funded by for-profit tech companies</td>
<td>$49 billion (2013)[^233]</td>
</tr>
<tr>
<td>Best Practices</td>
<td>Public disclosure</td>
<td>Collaboration with tech industry in evidence collection[^234]</td>
</tr>
</tbody>
</table>

[^229] Ibid., 64  
## Intermediate-Range Nuclear Force (INF) Treaty Investigative Process

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>US Bureau of Arms Control, Verification and Compliance (AVC)</td>
<td>- US and Russian governments, inter-governmental organizations that verify adherence to INF Treaty</td>
</tr>
<tr>
<td>Actions</td>
<td>Conduct on-site inspections and verifications, (^{235}) inter-state information exchange, (^{236}) reconnaissance and data analyses (^{237})</td>
<td></td>
</tr>
<tr>
<td>Authority</td>
<td>US Department of State</td>
<td></td>
</tr>
<tr>
<td>Structure</td>
<td>Centralized bureaucracy, government-to-government discussions and negotiations</td>
<td></td>
</tr>
<tr>
<td>Norms</td>
<td>INF Treaty provisioned protocols (^{238})</td>
<td></td>
</tr>
<tr>
<td>Attribution</td>
<td>Both nations have attributed treaty violations to the other nation (^{239})</td>
<td></td>
</tr>
<tr>
<td>Budget and Funding Source(s)</td>
<td>$32 million (2017) for compliance (^{240})</td>
<td>Funded by the US Department of State</td>
</tr>
<tr>
<td>Best Practices</td>
<td>Information exchange between nations</td>
<td>Process builds confidence between nations</td>
</tr>
<tr>
<td></td>
<td>Strong definitions section in the INF Treaty</td>
<td>Useful dispute resolution mechanism</td>
</tr>
</tbody>
</table>


\(^{236}\) Ibid.

\(^{237}\) Ibid.


## Malaysia Airlines Flight 17 (MH17) Crash Investigation

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Bellingcat, an online investigation hub, the media</td>
<td>- Dutch Safety Board (DSB)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Joint Investigation Team (JIT) member states (the Netherlands, Australia, Belgium, Malaysia, and Ukraine)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Public Prosecution Service (Dutch Ministry of Justice)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Online intelligence gathering</td>
<td>- Wide spectrum crash investigation(^2(^2(^2))) and information sharing</td>
</tr>
<tr>
<td></td>
<td>- Publishing of analyses(^2(^4(^1)))</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authority</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Reputational</td>
<td>- Dutch Government, JIT member states, UN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Structure</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Independent contributors,(^2(^4(^3))) ad-hoc, community-driven approach</td>
<td>- Bureaucratic</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Norms</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Rules of transparency, verifiability of data</td>
<td>- ICAO standards for evidence collection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribution</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Released findings after evidence collection and a review process(^2(^4(^4)))</td>
<td>- Attribution judgement was released by Public Prosecution Service(^2(^4(^5)))</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Budget and Funding Source(s)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Total budget unknown</td>
<td>- 36 million Euro (2014)(^2(^4(^8)))</td>
</tr>
<tr>
<td></td>
<td>- Funded through public pledges,(^2(^4(^6))) donations, and grants(^2(^4(^7)))</td>
<td>- Funded by the government of the Netherlands</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Best Practices</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Employment of information sharing mechanisms</td>
<td>- Inter-state collaboration and information exchange</td>
</tr>
<tr>
<td></td>
<td>- Engagement of independent international contributors and the pooling of multinational expertise</td>
<td>- Release of preliminary and final reports</td>
</tr>
<tr>
<td></td>
<td>- Adherence to evidence collection methods and standards</td>
<td>- Confidence building measures</td>
</tr>
</tbody>
</table>

---


\(^2\(^6\)\) "So how is Bellingcat funded?," whatthappenedtoflightmh17.com, March 25, 2016, [http://www.whatthappenedtoflightmh17.com/so-how-is-bellingcat-funded/](http://www.whatthappenedtoflightmh17.com/so-how-is-bellingcat-funded/).

\(^2\(^7\)\) Ibid., 111

### Mandiant’s APT1

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mandiant, private security firms, the media, academia[^249]</td>
<td></td>
</tr>
</tbody>
</table>

| Actions    | Investigate global attacks, attribute to specific individuals, share actionable information to prevent future attacks[^250] |        |

| Authority  | One of the ‘Top Four’ cybersecurity firms, composed of elite staff[^251] |        |

| Structure  | Centralized investigation, peer-review from other security firms and the media |        |

| Norms      | Full-disclosure, technical forensic norms, Information sharing, XML Schema[^252] |        |

| Attribution| Final attribution made in a report, details evidence collection and analysis[^253] |        |

| Budget and Funding Source(s) | Funded by private, for-profit firm |        |

| Best Practices | Public disclosure[^254] |        |
|                | Published analysis of evidence |        |
|                | Provided indicators:         |        |
|                | - Domains used by the attacking infrastructure, SSL certs, MDS hashes of APT1 malware, open source ‘indicators of compromise’[^255] |        |


[^254]: “APT1: Exposing One of China’s Cyber Espionage Units” on YouTube, accessed April 29, 2017, [https://www.youtube.com/watch?v=6p7FqSavSHo](https://www.youtube.com/watch?v=6p7FqSavSHo).

[^255]: Wade Williamson (2017) at 46.
### Mumbai Terrorist Attack Investigation

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- Intelligence agencies of US, United Kingdom, Australia, and Pakistan</td>
</tr>
<tr>
<td>Actions</td>
<td></td>
<td>- Conducted a criminal investigation, established cross-border intelligence sharing, and pressured Pakistan to become involved in the investigation.</td>
</tr>
<tr>
<td>Authority</td>
<td></td>
<td>- Ad-hoc and subjected to the legal authority of countries involved</td>
</tr>
<tr>
<td>Structure</td>
<td></td>
<td>- State integrated, non-bureaucratic</td>
</tr>
<tr>
<td>Norms</td>
<td></td>
<td>- Not peer-reviewed, but followed standard analysis of forensic evidence, low-degree of transparency, geographic representation</td>
</tr>
<tr>
<td>Attribution</td>
<td></td>
<td>- Released findings and specifically attributed attack to a terrorist group, and named individuals behind the planning.</td>
</tr>
<tr>
<td>Budget and Funding Source(s)</td>
<td></td>
<td>- Unknown</td>
</tr>
<tr>
<td>Best Practices</td>
<td></td>
<td>- Information and evidence sharing between multiple nations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Transnational data collection</td>
</tr>
</tbody>
</table>

---


257 Ibid., 115

258 Ibid., 115
## Sony Pictures Hack Investigation

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FireEye and Mandiant</td>
<td>FBI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Investigated source of attack</td>
<td>Investigated source of attack</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authority</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reputational – rose to prominence after implicating Chinese cyberespionage in 2013</td>
<td>US government</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Structure</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Five consulting offerings, “incident response and preparedness lifecycle”[^259]</td>
<td>Cyber division, 56 field offices with cyber teams 93 computer crimes task forces</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Partnerships with Department of Defense, Homeland Security[^260]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Norms</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Policies set out by FBI</td>
<td>US law</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribution</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No direct attribution</td>
<td>FBI concluded that North Korea is responsible for the attack[^261]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Budget and Funding Source(s)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$8.6 million (2016)[^262]</td>
<td>Budget for this investigation unknown</td>
</tr>
<tr>
<td></td>
<td>Funds raised primarily from venture investor</td>
<td>Funded by Department of Justice[^263]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Best Practices</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Called on for most major cybersecurity attacks</td>
<td>Exemplifies collaboration and cooperation across departments</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actors</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Symantec, VirusBlockAda, Kaspersky Labs, McAfee, other security firms, industry and geopolitical experts, the media</td>
<td>NSA, DHS, IAEA</td>
</tr>
</tbody>
</table>

| Actions | Worked on discovery, information sharing, technical analyses, and geopolitical analyses | NSA employees leaked classified information, IAEA Verified Iran’s compliance with the non-proliferation treaty, Provided context to Stuxnet attribution judgements |

| Authority | Reputational | US government, IAEA |

| Structure | Ad-hoc with Symantec and Kaspersky Labs taking leadership roles | Nation-state support was not active or structured in the investigation, All parties were only direct or indirect information providers |

| Norms | Information technology community best practices, transparency | The Statute of IAEA, information confidentiality practices and non-disclosure laws |

| Attribution | Final attributional judgements were drawn by media while the firms collected evidence, completed analyses | Confirmed already established attribution judgments |

| Budget and Funding Source(s) | Budget unknown, Each party funded independently | Total amount is unknown, Not clear whether NSA/DHS employees were compensated |

| Best Practices | Information sharing mechanisms, Confidence building, Pooling of multinational expertise, Evidence collection methods | Information retrieval methods from state entities |

---


269 Ibid., 126


Appendix 3: Proposed Budget

The table below summarizes the expected costs of the proposed organization. We break down the costs into six different categories, the Expert Investigation Committee, the Expert Review Committee, the Communications Committee, the Budget Committee, Outreach and Member Relations, and Infrastructure and Operations. The Executive Council will not be paid as their work is minimal while the reputational benefits are high.

The positions in the proposed organization are modelled after and chosen from previous investigative processes, large private corporations, and non-governmental organizations.

The Expert Investigation and Expert Review Committees will include both technical cybersecurity experts and geopolitical experts from academia and industry. These positions are modelled after major corporations such as Microsoft and Amazon who also have geopolitical experts working with or in technical cybersecurity teams to give context to the cyber environment.

The Expert Review Committee members will support the proposed organization on a part-time consulting basis. The Communications Committee will include public relations associates to provide updates in attribution investigations and disseminate attribution reports to the public. This committee will also house the legal team. The Outreach and Member Relations Committee will be responsible for the biannual meetings. Finally, the proposed organization will include staff for Infrastructure and Operations.

The one-time costs include initial technology purchases and office purchases in all six regions of the proposed organization. The miscellaneous operating expenses includes the maintenance and yearly costs of office space, supplies, and operations.

The salaries and costs have been calculated based on industry averages and comparable salaries of the associated positions. The infrastructure costs have also been calculated at office space prices in the respective regions.
Table 2: Proposed Budget for Year 1 and Subsequent Years

<table>
<thead>
<tr>
<th>Type of Costs</th>
<th>Position Name</th>
<th>Per position cost/year</th>
<th>Total cost/year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expert Investigation Committee</td>
<td>4 Industry Cyber Leads</td>
<td>$500,000</td>
<td>$2,000,000</td>
</tr>
<tr>
<td></td>
<td>12 Industry Cyber Experts</td>
<td>$300,000</td>
<td>$3,600,000</td>
</tr>
<tr>
<td></td>
<td>6 Geopolitical Leads</td>
<td>$500,000</td>
<td>$3,000,000</td>
</tr>
<tr>
<td></td>
<td>12 Geopolitical Analysts</td>
<td>$280,000</td>
<td>$3,360,000</td>
</tr>
<tr>
<td>Expert Review Committee</td>
<td>8 Part-time Cybersecurity Consultants</td>
<td>$150,000</td>
<td>$1,200,000</td>
</tr>
<tr>
<td></td>
<td>8 Part-time Geopolitical Experts</td>
<td>$150,000</td>
<td>$1,200,000</td>
</tr>
<tr>
<td>Communications Committee</td>
<td>1 Public Relations Director</td>
<td>$500,000</td>
<td>$500,000</td>
</tr>
<tr>
<td></td>
<td>5 Public Relations Associates</td>
<td>$160,000</td>
<td>$800,000</td>
</tr>
<tr>
<td></td>
<td>1 General Counsel</td>
<td>$500,000</td>
<td>$500,000</td>
</tr>
<tr>
<td></td>
<td>3 Attorneys</td>
<td>$320,000</td>
<td>$960,000</td>
</tr>
<tr>
<td>Budget Committee</td>
<td>1 Finance Director</td>
<td>$360,000</td>
<td>$360,000</td>
</tr>
<tr>
<td></td>
<td>4 Financial Administrators</td>
<td>$120,000</td>
<td>$480,000</td>
</tr>
<tr>
<td>Outreach &amp; Member Relations</td>
<td>Biannual Member Meetings</td>
<td>$2,000,000</td>
<td>$4,000,000</td>
</tr>
<tr>
<td></td>
<td>18 Outreach Coordinators</td>
<td>$120,000</td>
<td>$2,160,000</td>
</tr>
<tr>
<td>Infrastructure &amp; Operations</td>
<td>8 Administrative Positions</td>
<td>$160,000</td>
<td>$1,280,000</td>
</tr>
<tr>
<td></td>
<td>12 Server Administrators</td>
<td>$160,000</td>
<td>$1,920,000</td>
</tr>
<tr>
<td></td>
<td>Miscellaneous Operating Expenses</td>
<td></td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td>One-time infrastructure cost</td>
<td></td>
<td>$10,560,000</td>
</tr>
<tr>
<td>First Year Projected Budget</td>
<td></td>
<td></td>
<td>$38,880,000</td>
</tr>
<tr>
<td>Subsequent Years Projected Budget</td>
<td></td>
<td></td>
<td>$28,320,000</td>
</tr>
</tbody>
</table>
Bibliography

http://investingnews.com/daily/tech-investing/cybersecurity-investing/top-cyber-
security-companies/.

global-financial-report/.

“2016 Report on Adherence to and Compliance With Arms Control, Nonproliferation, and 
Disarmament Agreements and Commitments.” U.S. Department of State. Accessed April 

https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-
december-2014-sony-hack/.


icao/partnerships/Pages/default.aspx.

icao/partnerships/Pages/default.aspx.

“About Cyber Defence Centre | CCDCOE.” NATO Cooperative Cyber Defence Centre of 


“About Our Research.” Human Rights Watch, April 21, 2015. https://www.hrw.org/about-
our-research.


“Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament 

Aftergood, Steven. “Commercial Satellites as ‘National Technical Means.’” Federation of 
American Scientists, March 5, 2008. 
https://fas.org/blogs/secrecy/2008/03/commercial_satellites_as_natio/.

insider-trading-inquiry-tiger-asia-calls-it-quits/?_r=0.

icao/AirNavigationCommission/Pages/default.aspx.

Alperovitch, Dmitri. “Bears in the Midst: Intrusion into the Democratic National Committee ».” 
CROWDSTRIKE BLOG, June 15, 2016. https://www.crowdstrike.com/blog/bears-midst-
intrusion-democratic-national-committee/.

82

“An Outline of the FINRA Arbitration Process For Customer-Broker Disputes.” Smiley Bishop & 


“Approach and Standard.” Office of the Ombudsperson of the Security Council’s 1267 


https://www.youtube.com/watch?v=6p7FqSav6Ho.


“Asia Times Online: Korea News and Korean Business and Economy, Pyongyang News,” May 2, 

“‘Aurora’ Cyber Attackers Were Really Running Counter-Intelligence | CIO,” May 2, 2017.
http://www.cio.com/article/2386547/government/-aurora--cyber-attackers-were-really-running-counter-intelligence.html.

Ball, James. “Guardian Launches SecureDrop System for Whistleblowers to Share Files | 

Barrett, Devlin. “FBI Says North Korea Behind Sony Hack.” Wall Street Journal, December 19, 

Baruah, Amit. “Pakistan ‘Shared Mumbai Attacks Research with India’ - BBC News,” December 

BPR Administration, “BPR Interview: Citizens Lab Director Ronald Deibert,” Brown Political 

Bright, Arthur. “Estonia Accuses Russia of ‘Cyberattack.’” Christian Science Monitor, May 17, 

Broad, William J., and John Markoff, and David E. Sanger. "Israel Tests on Worm Called Crucial 
https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&ref=general&src=me&pagewanted=all.


https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/.


https://www.washingtonpost.com/world/report-ties-100-plus-cyber-attacks-on-us-computers-to-chinese-military/2013/02/19/2700228e-7a6a-11e2-9a75-dab0201670da_story.html?utm_term=.5cd49327297e.


“Results Confirm North Korea Sank Cheonan- Daily NK,” May 2, 2017. 


https://www.schneier.com/blog/archives/2015/03/attack_attribut_1.html.

Schneier, Bruce. “Click Here to Kill Everyone with the Internet of Things, we’re building a world-size robot. How are we going to control it?,” New York Magazine, (January, 2017)


https://www.csis.org/analysis/cyber-threat-information-sharing.