

THE HENRY M. JACKSON  
SCHOOL OF INTERNATIONAL STUDIES  

---

UNIVERSITY of WASHINGTON

# 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](mailto: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 21<sup>st</sup> 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.<sup>1</sup>

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.<sup>2</sup> 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.<sup>3</sup> 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.<sup>4</sup>

---

<sup>1</sup> For a general overview on the erosion of trust resulting from hacks and government surveillance see: Jack Goldsmith, “Toward Greater Transparency of National Security Legal Work.” *Jack Goldsmith*, May 6, 2015. <http://jackgoldsmith.org/toward-greater-transparency-of-national-security-legal-work/> and Marc Goodman, *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*. New York: Anchor Books, 2016.

<sup>2</sup> David A. Wheeler, and Gregory N. Larsen. “Techniques for Cyber Attack Attribution.” *Institute for Defense Analyses*, October 2003. <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859>.

<sup>3</sup> 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>

<sup>4</sup> John P. Carlin. “Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats.” *Harvard National Security Journal* Vol. 7. Harvard University, 2016. <https://docs.google.com/viewer?doce=1&url=https://lawfare.s3-us-west-2.amazonaws.com/staging/2016/Carlin%20FINAL.pdf>

While the need for attribution is clear, speed and integrity are key obstacles to the production of successful attribution judgements.<sup>5</sup> 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.<sup>6</sup>

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.<sup>7</sup> 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.<sup>8</sup> 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 organizations we evaluated were: 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, and the World Trade Organization's GATT Article XX.

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

---

<sup>5</sup> Bruce Schneier, "Attack Attribution and Cyber Conflict," *Schneier on Security*, 2015. Accessed May 25, 2017. [https://www.schneier.com/blog/archives/2015/03/attack\\_attribut\\_1.html](https://www.schneier.com/blog/archives/2015/03/attack_attribut_1.html).

<sup>6</sup> Healey, Jason. "Beyond Attribution: Seeking National Responsibility in Cyberspace." Atlantic Council, 2012. <http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace>.

<sup>7</sup> Carlin, 2016.

<sup>8</sup> 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

<b>Actors</b>	<i>Private Sector</i> - Company representatives, industry experts, independent academics
<b>Actions</b>	- Leads neutral, private sector investigations of major state-sponsored cyberattacks to determine attribution.
<b>Authority</b>	- Reputational
<b>Structure</b>	- 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
<b>Norms</b>	- Peer-review, high transparency, evidentiary framework
<b>Attribution</b>	- Investigation report articulates attribution - The Communications Committee disseminates attribution report, with full transparency, to mainstream news organizations
<b>Budget and Funding Source(s)</b>	- \$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. 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.

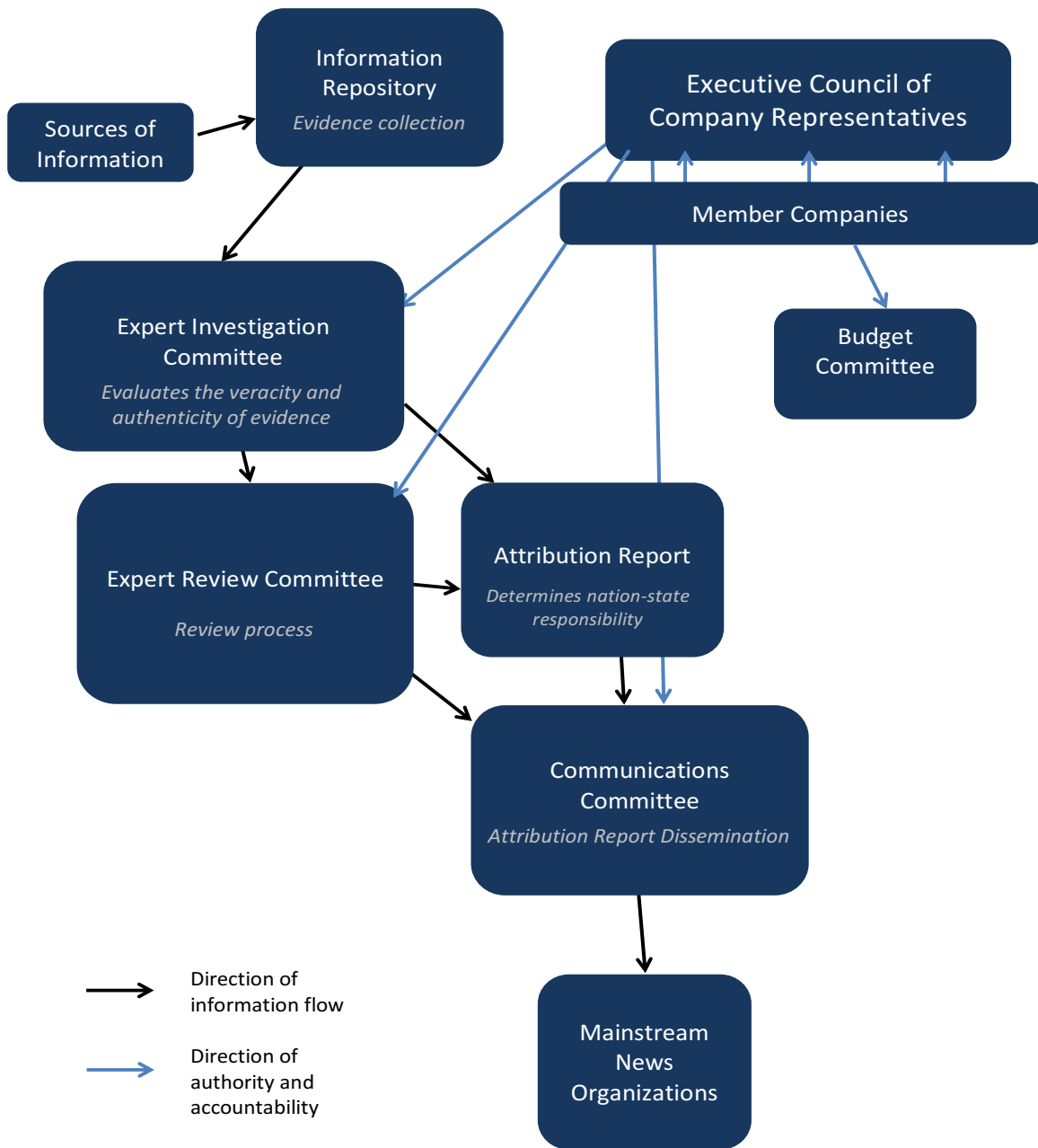


Figure 1: Organizational Chart

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

<b>Executive Summary</b> .....	<b>i</b>
The Attribution Challenge .....	i
Blueprint for an Attribution Organization .....	ii
<i>Table 1: Organizational Blueprint</i> .....	<i>iv</i>
<i>Figure 1: Organizational Chart</i> .....	<i>v</i>
<b>Introduction</b> .....	<b>1</b>
Blueprint for an Attribution Organization .....	3
<i>Table 1: Organizational Blueprint</i> .....	<i>5</i>
<i>Figure 1: Organizational Chart</i> .....	<i>7</i>
<i>Figure 2: Incorporation of Best Practices</i> .....	<i>8</i>
<b>Creating A Cyberattack Attribution Organization</b> .....	<b>9</b>
Mission .....	9
Methodology .....	11
<i>Actors</i> .....	<i>12</i>
<i>Actions</i> .....	<i>12</i>
<i>Authority</i> .....	<i>12</i>
<i>Structure</i> .....	<i>12</i>
<i>Norms</i> .....	<i>12</i>
<i>Attribution</i> .....	<i>12</i>
<i>Budgeting and Funding Sources</i> .....	<i>12</i>
<i>Figure 3: Spectrum of State Authority</i> .....	<i>13</i>
<b>Incorporating Best Practices</b> .....	<b>14</b>
Equitable Geographic Representation .....	14
<i>Equitable Geographic Distribution: Greenpeace, OPCW, and the Cheonan Joint Investigation Group</i> ..	<i>15</i>
<i>Adopting Equitable Geographical Representation</i> .....	<i>16</i>
Organizational Transparency .....	16
<i>Low Transparency Model: The Cheonan Joint Investigation Group</i> .....	<i>17</i>
<i>High Transparency Model: Mandiant’s APT1 Report</i> .....	<i>19</i>
<i>Adopting Transparency</i> .....	<i>20</i>
Stakeholder Outreach .....	20
<i>Stakeholder Outreach Models: OPCW and the Egmont Group</i> .....	<i>21</i>
<i>Adopting Stakeholder Outreach</i> .....	<i>22</i>
Internal Accountability .....	22
<i>Internal Accountability Models: UN ISIL and al-Qaida Sanctions Committee and the INF Treaty</i> .....	<i>23</i>
<i>Adopting of Internal Accountability</i> .....	<i>23</i>
Inclusion of Technical and Geopolitical Experts .....	24
<i>Expert Inclusion Models: The Cheonan Investigation and the IAEA</i> .....	<i>24</i>
<i>Adopting Expert Inclusion in Investigations</i> .....	<i>25</i>

Private Sector Membership.....	26
<i>Private Sector Membership Models: The Sony Hack Investigation and the Egmont Group</i> .....	26
<i>Adopting Private Sector Membership</i> .....	28
<b>The Design of the Proposed Organization .....</b>	<b>31</b>
Executive Council .....	31
Expert Investigation Committee .....	31
Expert Review Committee.....	32
Communications Committee .....	33
Budget Committee .....	33
Information Flow.....	34
<i>Figure 1: Organizational Chart</i> .....	35
<b>Challenges for the Proposed Organization .....</b>	<b>36</b>
Earning Public Trust.....	36
<i>Maintaining Independent Funding</i> .....	37
<i>Functioning as a Public Resource</i> .....	37
Cooperation among Competitors.....	38
<i>Incentivizing Cooperation through Access to Resources</i> .....	39
<i>Encouraging Cooperation through Privacy Assurances</i> .....	41
Industry Compliance with Organizational Norms .....	41
<i>Rationalist Behavior Theory</i> .....	42
<i>Constructivist Theory</i> .....	42
<i>Using Theory to Understand Compliance</i> .....	43
Legal Challenges of Information Sharing.....	44
<i>Automating Data Analysis</i> .....	44
Collecting Sensitive and Confidential Cyber Incident Information.....	45
<i>SecureDrop: A Tool for Anonymity and Sensitive Data Collection from the Public</i> .....	46
<i>Tearlines: A Mechanism for Receiving Government Information</i> .....	47
Methods of Information Sharing.....	48
<i>Adopting an Ad-Hoc Method of Exchange</i> .....	49
<i>Toward a Formalized Method of Exchange</i> .....	50
Sharing Information with China and Russia .....	51
<i>Engaging the Private Sector</i> .....	52
<b>Conclusion.....</b>	<b>54</b>
<b>Appendix 1: International Organizations .....</b>	<b>55</b>
Amnesty International .....	56
Citizen Lab .....	57
Egmont Group of Financial Intelligence Units .....	58
European Financial Coalition Against Child Pornography (EFCACP).....	59
The Financial Industry Regulatory Authority (FINRA).....	60
Greenpeace .....	61

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
<b>Appendix 2: Investigative Processes .....</b>	<b>70</b>
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
<b>Appendix 3: Proposed Budget.....</b>	<b>80</b>
<i>Table 2: Proposed Budget for Year 1 and Subsequent Years .....</i>	<i>81</i>
<b>Bibliography .....</b>	<b>82</b>

# Introduction

In April 2007, Estonia was cut off from the Internet.<sup>9</sup> 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."<sup>10</sup> 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.<sup>11</sup> 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

---

<sup>9</sup> Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, accessed May 17, 2017, <https://www.wired.com/2007/08/ff-estonia/>.

<sup>10</sup> "War in the fifth domain. Are the mouse and keyboard the new weapons of conflict?," *The Economist*, July 1, 2010, accessed May 17, 2017, <http://www.economist.com/node/16478792>

<sup>11</sup> Arthur Bright, "Estonia accuses Russia of 'cyberattack'," *CSMonitor.com*, May 7, 2017, accessed May 17, 2017, <http://www.csmonitor.com/2007/0517/p99s01-duts.html>; Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian*, May 16, 2007, accessed May 17, 2017, <https://www.theguardian.com/world/2007/may/17/topstories3.russia>; "The 2007 Estonian Cyberattacks: New Frontiers in International Conflict," *Cyber War Harvard Law Blog*, December 21, 2012, accessed May 17, 2017, <https://blogs.harvard.edu/cyberwar43z/2012/12/21/estonia-ddos-attackrussian-nationalism/>; "Estonia Fines Man for 'Cyber War,'" *BBC.com*, January 25, 2008. Accessed May 2017 at <http://news.bbc.co.uk/2/hi/technology/7208511.stm>

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.<sup>12</sup>

Attribution, or the identification of an attacker, is a challenge at the core of many cybersecurity problems.<sup>13</sup> 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.<sup>14</sup> 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.<sup>15</sup>

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.<sup>16</sup> The attacker's invisibility is a principal cause for the deluge of cyber threats because it makes his or her actions relatively cost-free.<sup>17</sup>

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,

---

<sup>12</sup> Bruce Schneier, "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, <http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html>

<sup>13</sup> David A. Wheeler, and Gregory N. Larsen. "Techniques for Cyber Attack Attribution." Institute for Defense Analyses, October 2003, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859>

<sup>14</sup> Herbert Lin. "Attribution of Malicious Cyber Incidents: From Soup to Nuts," *Journal of International Affairs* 70(1) (2016): 75-137,11.; David Clark and Susan Landau. "Untangling Attribution." Massachusetts Institute of Technology, 2011. <http://static.cs.brown.edu/courses/csci1950-p/sources/lec12/ClarkandLandau.pdf>; Jason Healey. "Beyond Attribution: Seeking National Responsibility in Cyberspace." Atlantic Council, 2012. <http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace>.

<sup>15</sup> 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>

<sup>16</sup> Clark and Landau, 2011.

<sup>17</sup> John P. Carlin. "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats." Harvard National Security Journal Vol. 7. Harvard University, 2016. <https://docs.google.com/viewer?doce=1&url=https://lawfare.s3-us-west-2.amazonaws.com/staging/2016/Carlin%20FINAL.pdf>.

signals intelligence, and geopolitics.<sup>18</sup> With this information, experts can produce an attribution judgment resolving the basic question of responsibility.<sup>19</sup> 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.<sup>20</sup>

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.

## 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,

---

<sup>18</sup> Lin, 2016, 11.

<sup>19</sup> Healey, 2012.

<sup>20</sup> Carlin, 2016.

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, and the World Trade Organization's GATT Article XX.

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

<b>Actors</b>	<i>Private Sector</i> - Company representatives, industry experts, independent academics
<b>Actions</b>	- Leads neutral, private sector investigations of major state-sponsored cyberattacks to determine attribution.
<b>Authority</b>	- Reputational
<b>Structure</b>	- 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
<b>Norms</b>	- Peer-review, high transparency, evidentiary framework
<b>Attribution</b>	- Investigation report articulates attribution - The Communications Committee disseminates attribution report, with full transparency, to mainstream news organizations
<b>Budget and Funding Source(s)</b>	- \$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.

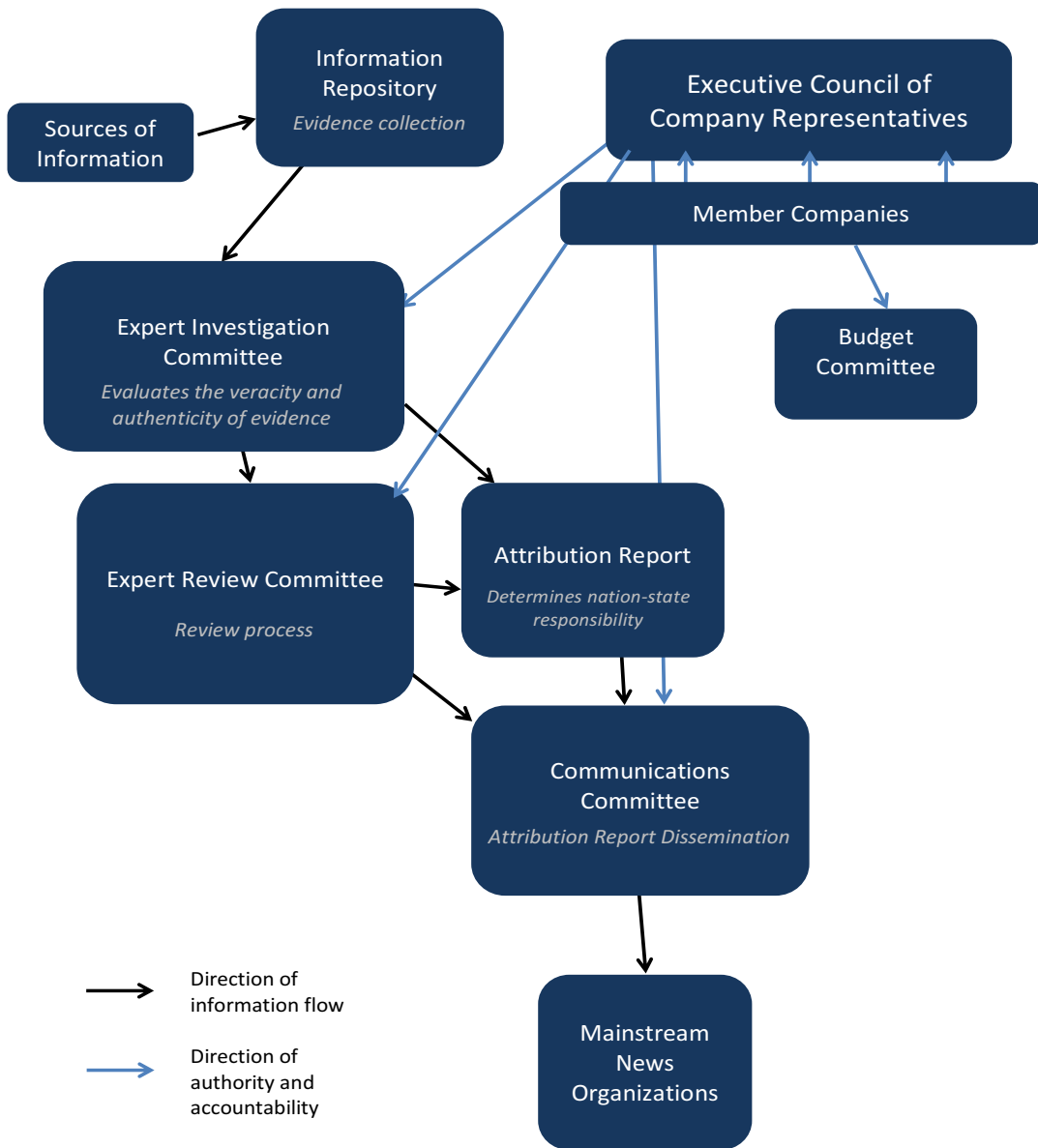


Figure 1: Organizational Chart

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.



Figure 2: Incorporation of Best Practices

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.<sup>21</sup> 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.<sup>22</sup> 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

---

<sup>21</sup> Bruce Schneier, "Attack Attribution and Cyber Conflict," *Schneier On Security*, March 9, 2015, accessed May 23, 2017, [https://www.schneier.com/blog/archives/2015/03/attack\\_attribut\\_1.html](https://www.schneier.com/blog/archives/2015/03/attack_attribut_1.html)

<sup>22</sup> 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.<sup>23</sup>

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.<sup>24</sup> 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 bolster 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,

---

<sup>23</sup> Jeffrey Hunker, Bob Hutchinson and Jonathan Margulies, "Role and Challenges for Sufficient Cyber-Attack Attribution," Institute for Information Infrastructure Protection (2008), accessed May 17, 2017, <http://www.scis.nova.edu/%7Ecannady/ARES/hunker.pdf>

<sup>24</sup> "Cyber-Security task Force: Public-Private Information Sharing," Bipartisan Policy Review (2012), <http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Public-Private%20Information%20Sharing.pdf>.

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 organizations we evaluated were: Amnesty International, 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, and the World Trade Organization's GATT Article XX.

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.

Bureaucratic				Ad-hoc	
<u>International Organizations</u> <ul style="list-style-type: none"> <li>• Formal authority</li> <li>• Nonprofit</li> <li>• Member state and private funding</li> <li>• Ratified treaties</li> </ul>				<u>International Investigations</u> <ul style="list-style-type: none"> <li>• Private Enterprises</li> <li>• Informal authority</li> <li>• For-profit mission driven strategies</li> <li>• Ad-hoc information-sharing</li> </ul>	
Tools <ul style="list-style-type: none"> <li>• Bilateral, multilateral treaties</li> <li>• Agreements between governments</li> <li>• Partnerships among governmental agencies and NGO institutions</li> </ul>					
<i>Greater number of participants, less specific</i>				<i>Fewer number of participants, more specific</i>	
Examples: <ul style="list-style-type: none"> <li>• IAEA</li> <li>• UN Sanctions</li> <li>• WTO Article XX</li> <li>• Amnesty International</li> <li>• NATO CCDCOE</li> </ul>	Examples: <ul style="list-style-type: none"> <li>• ILO</li> <li>• Egmont Group</li> <li>• EFCACP</li> </ul>	Examples: <ul style="list-style-type: none"> <li>• Mumbai Investigation</li> <li>• OPCW</li> <li>• ICAO</li> </ul>	Examples: <ul style="list-style-type: none"> <li>• Google's 'Operation Aurora'</li> <li>• Cheonan JIG</li> </ul>	Examples: <ul style="list-style-type: none"> <li>• DNC Hack</li> </ul>	Examples: <ul style="list-style-type: none"> <li>• Stuxnet</li> <li>• Mandiant APT1</li> </ul>

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.<sup>25</sup> 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.<sup>26</sup> 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.<sup>27</sup>

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

---

<sup>25</sup> "Greenpeace structure and organization." *Greenpeace International 2017*, accessed April 30, 2017.

<http://www.greenpeace.org/international/en/about/how-is-greenpeace-structured/>

<sup>26</sup> "Membership and Functions," *Organization for the Prohibition of Chemical Weapons*, Accessed April 30, 2017, <https://www.opcw.org/about-opcw/executive-council/membership-and-functions/>

<sup>27</sup> "Rules and Procedure for the Scientific Advisory Board and Temporary Working Groups of Scientific Experts," *Organization for the Prohibition of Chemical Weapons*. Accessed May 10, 2017.

ability to produce credible findings to the international community.<sup>28</sup> 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.<sup>29</sup> South Korea's deliberate internationalization of the investigation made it harder for North Korea to dismiss the accusations of the investigation being politically motivated.<sup>30</sup> 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

---

<sup>28</sup> "Security Council Condemns Attack on Republic of Korea Naval Ship 'Cheonan', Stresses Need to Prevent Further Attacks, Other Hostilities in Region," *United Nations*. July 9, 2010.

<sup>29</sup> "Letter Dated 4 June 2010 from the Permanent Representative of the Republic of Korea to the United Nations Address to the President of the Security Council." (United Nations Security Council, June 4, 2010).

<sup>30</sup> Mark Landler, "Diplomatic Storm Brewing Over Korean Peninsula," *The New York Times*, May 19, 2010, accessed May 17, 2017, <http://www.nytimes.com/2010/05/20/world/asia/20diplo.html>

considered valid and for ensuring that private sector companies will join the organization.<sup>31</sup> 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 *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 *Cheonan* Joint Investigation Group

The *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 *Cheonan* sank near the Northern Limit Line, a *de facto* jurisdictional border with North Korea, killing 46 servicemen.<sup>32</sup> The South Korean government withheld formal indictments immediately after the sinking, although the incident heightened tensions between the two Koreas.<sup>33</sup> 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.<sup>34</sup> However, the investigation's secretive process was highly controversial, particularly among other forensic scientists and the public.<sup>35</sup> 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.<sup>36</sup>

---

<sup>31</sup> Neil Patel, "Why a Transparent Culture Is Good for Business," *Fast Company*, October 9, 2014, <https://www.fastcompany.com/3036794/why-a-transparent-culture-is-good-for-business>

<sup>32</sup> Landler, 2010.

<sup>33</sup> Landler, 2010.

<sup>34</sup> "Investigation Result on the Sinking of ROKS "Cheonan," The Joint Military-Civilian Investigation Group (2010), accessed May 17, 2017, [http://news.bbc.co.uk/nol/shared/bsp/hi/pdfs/20\\_05\\_10jigreport.pdf](http://news.bbc.co.uk/nol/shared/bsp/hi/pdfs/20_05_10jigreport.pdf)

<sup>35</sup> David Cyranoski, "Controversy over South Korea's sunken ship," *Nature Journal*, July 14, 2010, accessed May 22, 2017, <http://www.nature.com/news/2010/100708/full/news.2010.343.html>

<sup>36</sup> Harvey Morris, "N Korea escapes blame over ship sinking," *Financial Times*, July 9, 2017, accessed May 22, 2017, <https://www.ft.com/content/4208c344-8b6e-11df-ab4d-00144feab49a>.

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.<sup>37</sup> 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.<sup>38</sup>

Subsequent research from scientists further raised the possibility that the sinking was caused by other factors.<sup>39</sup> An oversight board for the South Korean military accused the investigation of analyzing information distorted by the South Korean naval leaders.<sup>40</sup> Critics speculated that the reason for not disclosing information is to protect the South Korean army from liability.<sup>41</sup> 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.<sup>42</sup>

The *Cheonan* example illustrates why attribution investigations of state-sponsored attacks should prioritize transparency and provide an open peer-review process.<sup>43</sup> 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

---

<sup>37</sup> Barbara Demick and John M. Glionna, "Doubts surface on North Korea's role in ship sinking," Los Angeles Times, July 23, 2010, accessed May 22, 2017, <http://articles.latimes.com/2010/jul/23/world/la-fg-korea-torpedo-20100724>.

<sup>38</sup> David Cyranoski, "Controversy over South Korea's sunken ship," *Nature Journal*, July 14, 2010, accessed May 22, 2017, <http://www.nature.com/news/2010/100708/full/news.2010.343.html> and Seunghun Lee and J.J. Suh, "Policy Forum 10-039: Rush to Judgment: Inconsistencies in South Korea's Cheonan Report", NAPSNet Policy Forum, July 15, 2010, <http://nautilus.org/napsnet/napsnet-policy-forum/rush-to-judgment-inconsistencies-in-south-koreas-cheonan-report/>

<sup>39</sup> Hwang Su Kim and Mauro Caresta, "What Really Caused the ROKS Cheonan Warship Sinking?" *Advances in Acoustics and Vibration* (2014), accessed May 22, 2017, <https://www.hindawi.com/journals/aav/2014/514346/>.

<sup>40</sup> Demick and Glionna, 2010.

<sup>41</sup> Ibid.

<sup>42</sup> "Ex-Pres. Secretary Sued for Spreading Cheonan Rumors," *The Dong-A Ilbo* (English Edition), May 8, 2010, accessed May 22, 2017, <http://english.donga.com/List/3/all/26/264989/1>

<sup>43</sup> "Most S. Koreans Skeptical About Cheonan Findings, Survey Shows," *The Chosun Ilbo* (English Edition), September 8, 2010, accessed May 17, 2017, [http://english.chosun.com/site/data/html\\_dir/2010/09/08/2010090800979.html](http://english.chosun.com/site/data/html_dir/2010/09/08/2010090800979.html)

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.<sup>44</sup> The importance of Mandiant's report comes from the breadth of evidence disclosed to the public and engagement with the press.<sup>45</sup> 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.<sup>46</sup> 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.<sup>47</sup>

In addition, Mandiant shared the technical tools and procedures used to gather evidence and explained in nontechnical language the method of analysis.<sup>48</sup> In doing so, Mandiant bolstered

---

<sup>44</sup> Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," accessed April 29, 2017, <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>

<sup>45</sup> David E. Sanger, David Barboza and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," New York Times, February 29, 2013, accessed April 29, 2017, <https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>

<sup>46</sup> Benjamin Wittes, "Mandiant Report on 'APT 1'," Lawfare.org, February 20, 2013, accessed April 29, 2017, <https://lawfareblog.com/mandiant-report-apt1>; William Wan and Ellen Nakashima, "Report ties cyberattacks on U.S. computers to Chinese military," Washington Post, January 19, 2013, accessed April 29, 2017, [https://www.washingtonpost.com/world/report-ties-100-plus-cyber-attacks-on-us-computers-to-chinese-military/2013/02/19/2700twenty-two8e-7a6a-11e2-9a75-dab0201670da\\_story.html](https://www.washingtonpost.com/world/report-ties-100-plus-cyber-attacks-on-us-computers-to-chinese-military/2013/02/19/2700twenty-two8e-7a6a-11e2-9a75-dab0201670da_story.html)

<sup>47</sup> Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," accessed April 29, 2017, <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>

<sup>48</sup> Wade Williamson, "Lessons from Mandiant's APT1 Report," SECURITY WEEK, February 29, 2013, accessed April 29, 2017, <http://www.securityweek.com/lessons-mandiant%E2%80%99s-apt1-report>

the credibility of its attribution judgment by allowing extensive peer-review and public discussion.<sup>49</sup> 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

---

<sup>49</sup> Sanger, Barboza, and Perlroth, 2013.

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.<sup>50</sup> 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.<sup>51</sup> 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.<sup>52</sup> 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.

---

<sup>50</sup> "Suggested Best Practices for Industry Outreach Programs to Stakeholders" (Federal Energy Regulatory Commission, July 2015), <https://www.ferc.gov/industries/gas/enviro/guidelines/stakeholder-brochure.pdf>; "Create a Strategic Outreach Campaign to Add Value to Your Organization," *Prowl*, May 23, 2011, <http://prowlpublicrelations.blogspot.com/2011/06/create-strategic-outreach-campaign-to.html?m=0>.

<sup>51</sup> "OPCW Calendar of Events," *Organization for the Prohibition of Chemical Weapons*, n.d., <https://www.opcw.org/events-calendar/>.

<sup>52</sup> "Egmont Group Communication Strategy," *Egmont Group of Financial Intelligence Units*, (2015).

## 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 data 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 bolster 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.<sup>53</sup> The Ombudsperson provides detailed analysis and observations on all information relevant to a sanctions appeal before providing the Committee with a recommendation on delisting.<sup>54</sup> 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.<sup>55</sup>

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.<sup>56</sup> 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.<sup>57</sup>

## 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

---

<sup>53</sup> "Approach and Standard," *Office of the Ombudsperson of the Security Council's 1267 Committee*, n.d., <https://www.un.org/sc/suborg/en/ombudsperson/approach-and-standard>

<sup>54</sup> Ibid.

<sup>55</sup> "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.

<sup>56</sup> Amy F. Woolf, "Russian Compliance with the Intermediate Range Nuclear Forces (INF) Treaty: Background and Issues for Congress" *Congressional Research Service*, (2017).

<sup>57</sup> 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.<sup>58</sup> 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.<sup>59</sup> 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

---

<sup>58</sup> "Security Council Condemns Attack on Republic of Korea Naval Ship 'Cheonan', Stresses Need to Prevent Further Attacks, Other Hostilities in Region | Meetings Coverage and Press Releases" United Nations Security Council (2010), accessed May 16, 2017, <https://www.un.org/press/en/2010/sc9975.doc.htm>

<sup>59</sup> "Inspection and Enforcement by the Regulatory Body," 4.1.3.2. Methods of inspection. Accessed May 11, 2017. <https://www.iaea.org/ns/tutorials/regcontrol/inspect/insp4132.htm>

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.<sup>60</sup> 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.<sup>61</sup> 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.

---

<sup>60</sup> "Update on Sony Investigation," Press Release, Federal Bureau of Investigation, accessed May 23, 2017, <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>.

<sup>61</sup> Financial Action Task Force. "INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION." FAFTA/OECD, 2013. [http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF\\_Recommendations.pdf](http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

## 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.<sup>62</sup> An expected \$3 trillion in costs by 2020 will be attributed to cyber crime.<sup>63</sup> 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.<sup>64</sup> This diverse array of reporting entities provides Financial Intelligence Units with a comprehensive database of pertinent information

---

<sup>62</sup> Riley Walters, “Cyber Attacks on U.S. Companies Since November 2014,” The Heritage Foundation, accessed May 23, 2017, <http://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014>

<sup>63</sup> Protecting and Defending against Cyberthreats in Uncertain Times | USA 2017 | RSA Conference,” accessed May 23, 2017, <http://www.rsaconference.com/events/us17/agenda/sessions/7577-keynote-speaker-brad-smith-president-and-chief>.

<sup>64</sup> International Monetary Fund and World Bank, “Financial Intelligence Units: An Overview,” 2004, <https://www.imf.org/external/pubs/ft/FIU/fiu.pdf>

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.<sup>65</sup> 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

---

<sup>65</sup> J.E. Messerschmidt, "Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm," *Columbia Journal of Transnational Law*, Vol. 52, No. 1, p. 293 and Neal Katyal, "Community Self-Help," *Journal of Law, Economics and Policy*, Vol. 1, (2005), accessed may 17, 2017, <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1532&context=facpub>

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.

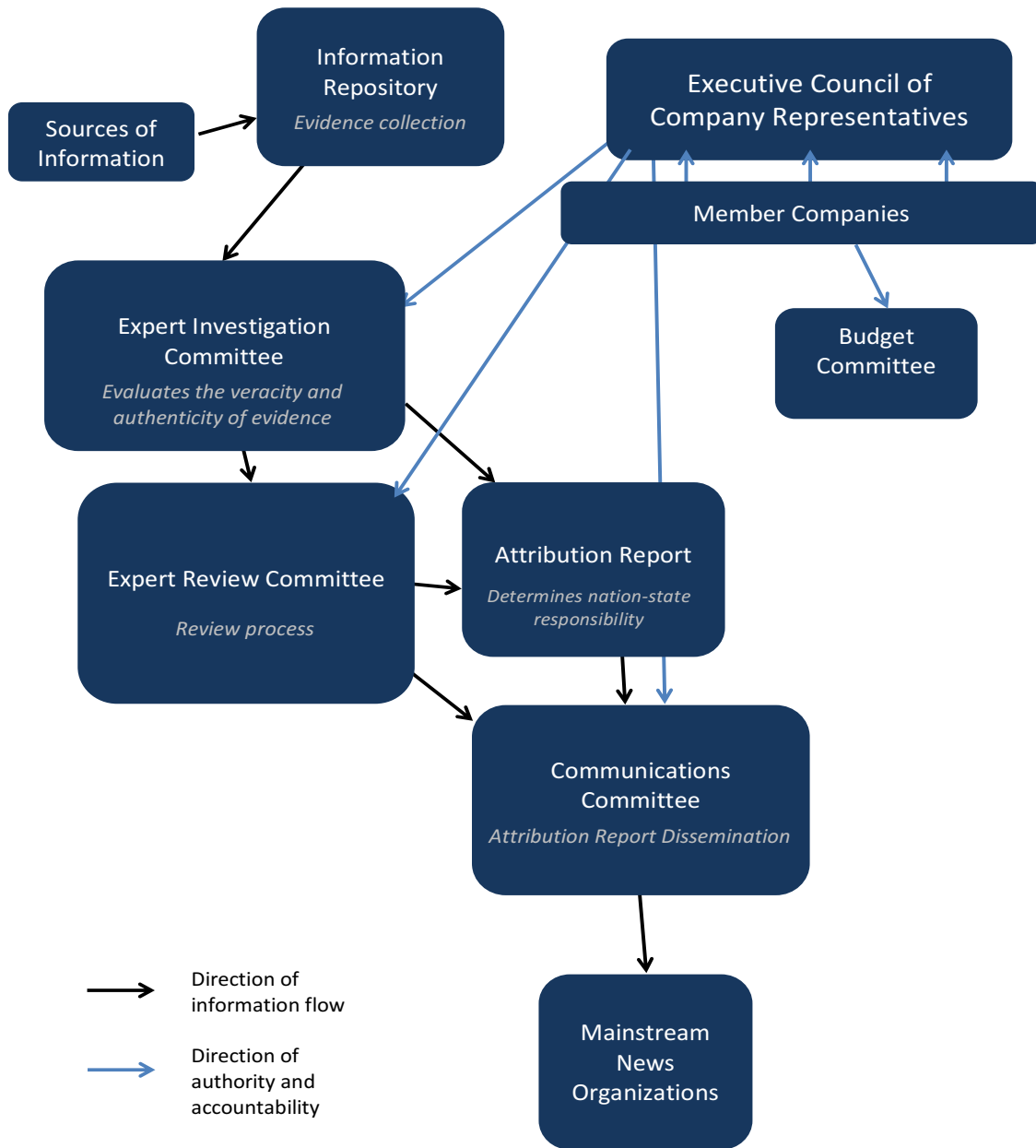


Figure 1: Organizational Chart

# 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.<sup>66</sup> 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.<sup>67</sup> Additionally, Greenpeace is responsible for impactful environmental campaigns, ranging from initiatives to stop drilling in the Arctic and stopping the flow toxic waste into the ocean.<sup>68</sup> 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

---

<sup>66</sup> "Who We Are." *Greenpeace International*. Accessed May 17, 2017. <http://www.greenpeace.org/international/en/about/our-mission/>

<sup>67</sup> "Greenpeace structure and organization." *Greenpeace International*. 2017. Accessed May 9, 2017.

<http://www.greenpeace.org/international/en/about/how-is-greenpeace-structured/>

<sup>68</sup> "Who We Are," 2017.

increasingly controversial, and nuclear energy is also highly technical, often too complex for the public to understand, further exacerbating mistrust in its use.<sup>69</sup> 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.<sup>70</sup> 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

---

<sup>69</sup> Black, Richard. "Nuclear Power 'Gets Little Public Support Worldwide.'" *BBC News*, November 25, 2011, sec. Science & Environment. <http://www.bbc.com/news/science-environment-15864806>

<sup>70</sup> IAEA. "Building Public Trust in Nuclear Power." International Atomic Energy Agency, March 2013. <https://www.iaea.org/sites/default/files/publications/magazines/bulletin/bull54-1/54104711212.pdf>

company to identify and patch every cybersecurity vulnerability arising in a single network.<sup>71</sup> 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.<sup>72</sup>

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.<sup>73</sup> 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.<sup>74</sup>

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.<sup>75</sup> Examples of the Egmont Group's resources

---

<sup>71</sup> Gagnon, Gary. "Why Businesses Should Share Intelligence About Cyber Attacks." *Harvard Business Review*, June 13, 2013.

<sup>72</sup> Gagnon, 2013.

<sup>73</sup> "Financial Intelligence Units (FIUs) - The Egmont Group."

<sup>74</sup> International Monetary Fund, and World Bank. "Financial Intelligence Units: An Overview," 2004.

<https://www.imf.org/external/pubs/ft/FIU/fiu.pdf>

<sup>75</sup> International Monetary Fund and World Bank, 2004.

include yearly plenaries and communiqués 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.<sup>76</sup> 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.<sup>77</sup> 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 the 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.

---

<sup>76</sup> "Public Statements and Communiqués - The Egmont Group." Accessed April 3, 2017. <https://www.egmontgroup.org/en/document-library/9>.

<sup>77</sup> 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.<sup>78</sup> In addition to working with Symantec, Kaspersky Lab also worked with other competing security firms such as McAfee, and collaborated with a range of industry and geopolitical experts to approach the investigation.<sup>79</sup> 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.<sup>80</sup> 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

---

<sup>78</sup> Kim Zetter, "How digital detectives deciphered Stuxnet, the most menacing malware in history," *WIRED*, July 11, 2011, accessed May 1, 2017, <https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/>.

<sup>79</sup> David Kushner, "The Real Story of Stuxnet: How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program," *IEEE Spectrum*, February 26, 2013, accessed May 1, 2017, <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

<sup>80</sup> 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.<sup>81</sup> 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.<sup>82</sup> 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.<sup>83</sup> 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

---

<sup>81</sup> See e.g. Harold Hongju Koh, "Why Do Nations Obey International Law?," Yale Faculty Scholarship Press (1997), accessed May 23, 2017, [http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2897&context=fss\\_papers](http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2897&context=fss_papers).

<sup>82</sup> Abram Chayes and Antonia Handler Chayes, "The New Sovereignty: Compliance with International Regulatory Agreements," *Harvard University Press* (1998).

<sup>83</sup> Doug Gross, "Google vs. China: Free speech, finances or both?," CNN, January 13, 2010, accessed May 11, 2017, <http://www.cnn.com/2010/TECH/01/13/google.china.analysis/index.html>

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.<sup>84</sup> 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.<sup>85</sup> Therefore, an organizational model based on discourse, persuasion, and cooperation, rather than coercion will lead to accordance with an international organization's rules.<sup>86</sup>

### 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.

---

<sup>84</sup> Harold Hongju Koh, "Why Do Nations Obey International Law?," Yale Faculty Scholarship Press (1997), accessed May 23, 2017, [http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2897&context=fsf\\_papers](http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2897&context=fsf_papers).

<sup>85</sup> Koh, 1997.

<sup>86</sup> Abram Chayes and Antonia Handler Chayes, "The New Sovereignty: Compliance with International Regulatory Agreements," *Harvard University Press* (1998).

## 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,<sup>87</sup> 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,<sup>88</sup> while Article 8 of the European Convention on Human Rights cites privacy rights as a reason to restrict data sharing.<sup>89</sup>

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.<sup>90</sup> In this position, it collects information on market

---

<sup>87</sup> Chris Johnson et al, "Guide to Cyber Threat Information Sharing," *National Institute of Standards and Technology (NIST)* (2016), available at: <http://dx.doi.org/10.6028/NIST.SP.800-150>.

<sup>88</sup> "International Covenant on Civil and Political Rights," *United Nations General Assembly* (1966), accessed May 17, 2017, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>.

<sup>89</sup> "Convention for the Protection of Human Rights and Fundamental Freedoms Rome," (1950), accessed May 17, 2017, <https://rm.coe.int/1680063765>.

<sup>90</sup> "About FINRA," *finra.org*, accessed May 1, 2017. <https://www.finra.org/about>; Carrie Johnson, "SEC Approves One Watchdog For Brokers Big and Small," *The Washington Post*, July 27, 2007, Page D02., accessed May 2, 2017, [http://www.washingtonpost.com/wp-dyn/content/article/2007/07/27/AR2007072700108\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2007/07/27/AR2007072700108_pf.html).

prices, equity trading, and other key variables in a centralized database.<sup>91</sup> 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.<sup>92</sup> 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.<sup>93</sup>

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.<sup>94</sup> Privacy will be further protected by establishing formal norms and procedures for the organization's gathering, sharing, and preserving evidence.<sup>95</sup>

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.<sup>96</sup> 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

---

<sup>91</sup> "Technology | FINRA.org," accessed May 16, 2017, <https://www.finra.org/about/technology>.

<sup>92</sup> "Technology | FINRA.org"

<sup>93</sup> Denise Zheng and James Lewis, "Cyber Threat Information Sharing," *Center for Strategic and International Studies* (2015), accessed May 17, 2017, <https://www.csis.org/analysis/cyber-threat-information-sharing>.

<sup>94</sup> Chris Johnson et al, 2016.

<sup>95</sup> Chris Johnson et al, 2016.

<sup>96</sup> Chris Johnson et al, 2016.

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.<sup>97</sup>

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

---

<sup>97</sup> WashPostPR, "Q&A about SecureDrop on The Washington Post," *The Washington Post*, June 5, 2014, accessed May 23, 2017, [https://www.washingtonpost.com/pr/wp/2014/06/05/qa-about-securedrop-on-the-washington-post/?utm\\_term=.75a18f73a812](https://www.washingtonpost.com/pr/wp/2014/06/05/qa-about-securedrop-on-the-washington-post/?utm_term=.75a18f73a812).

whistleblowers to confidentially share information and communicate with journalists.<sup>98</sup> 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.<sup>99</sup> 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.<sup>100</sup> 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.”<sup>101</sup> 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.”<sup>102</sup>

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

---

<sup>98</sup> James Ball, “Guardian launches SecureDrop system for whistleblowers to share files,” June 5, 2014, accessed May 23, 2017, <https://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents>.

<sup>99</sup> Ball, 2014.

<sup>100</sup> Trevor Timm, “SecureDrop Undergoes Second Security Audit,” *Freedom of the Press Foundation*, January 20, 2014, accessed May 23, 2017, <https://freedom.press/news-advocacy/securedrop-undergoes-second-security-audit/>.

<sup>101</sup> “Intelligence Community Directive 209-Tearline Production and Dissemination” (Office of the Director of National Intelligence, September 12, 2012): 2.

<sup>102</sup> “Intelligence Community Directive 209-Tearline Production and Dissemination,” 2012.

investigation.<sup>103</sup> 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.<sup>104</sup> 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.<sup>105</sup> 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.<sup>106</sup> 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.<sup>107</sup> It is not uncommon for an ad-hoc model to lay the groundwork for a more formalized method of information sharing in the future.<sup>108</sup>

---

<sup>103</sup> Amit Baruah, "Pakistan 'Shared Mumbai Attacks Research with India' - BBC News," December 4, 2010, <http://www.bbc.com/news/world-south-asia-11917514>.

<sup>104</sup> Cristin Goodwin and J. Paul Nicholas, "A Framework for Cybersecurity Information Sharing and Risk Reduction" (Microsoft, January 26, 2015), <https://www.microsoft.com/en-us/download/details.aspx?id=45516>.

<sup>105</sup> Ibid.

<sup>106</sup> Ibid.

<sup>107</sup> Ibid.

<sup>108</sup> 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 motivated<sup>109</sup> and originated in Pakistan with the perpetrators having close ties to Pakistani intelligence.<sup>110</sup> 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.

---

<sup>109</sup> Fire Eye, "APT 28: A Window Into Russia's Cyber Espionage Operations?," Intelligence Report, (October 2014).

<sup>110</sup> Sebastian Rotella, James Glanz, and David E. Sanger, "In 2008 Mumbai Attacks, Piles of Spy Data, but an Uncompleted Puzzle - ProPublica," *Pro Publica*, December 21, 2014, <https://www.propublica.org/article/mumbai-attack-data-an-uncompleted-puzzle>.

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.<sup>111</sup> 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.<sup>112</sup> These

---

<sup>111</sup> NATO, "About Cyber Defence Centre | CCDCOE," NATO Cooperative Cyber Defence Centre of Excellence, accessed April 30, 2017, <https://ccdcoe.org/about-us.html>

<sup>112</sup> "Tallinn Manual Process | CCDCOE," accessed May 4, 2017, <https://ccdcoe.org/tallinn-manual.html>.

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.<sup>113</sup> Furthermore, Chinese technology companies tend to adhere to the government's policies because they are financially rewarded for compliance with the state.<sup>114</sup> 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,

---

<sup>113</sup> Zach Warren, "Are you ready for the new China Cybersecurity Law?," *Inside Counsel*, February 28, 2017, accessed May 17, 2017, <http://www.insidecounsel.com/2017/02/28/are-you-ready-for-the-new-china-cybersecurity-law?ref=footer-news>.

<sup>114</sup> Hauke Johannes Gierow, "Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses," *MERICs*, April 22, 2015, accessed May 17, 2017, [http://www.merics.org/fileadmin/templates/download/china-monitor/150407\\_MERICs\\_China\\_Monitor\\_twenty-two\\_en.pdf](http://www.merics.org/fileadmin/templates/download/china-monitor/150407_MERICs_China_Monitor_twenty-two_en.pdf).

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.<sup>115</sup> 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.<sup>116</sup> Thus, Kaspersky Lab has scaled back significantly on its cooperation with non-Russian partners.<sup>117</sup>

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.<sup>118</sup> Chinese

---

<sup>115</sup> Dan Goodin, "Kaspersky Lab's top investigator reportedly arrested in treason probe," *ArsTechnica*, January 25, 2017, accessed May 17, 2017, <https://arstechnica.com/security/2017/01/kaspersky-labs-top-investigator-reportedly-arrested-in-treason-probe/>.

<sup>116</sup> Corey Flintoff, "Kaspersky Lab: Based in Russia, Doing Cybersecurity in the West," *NPR*, August 10, 2015, accessed May 17, 2017, <http://www.npr.org/sections/alltechconsidered/2015/08/10/431247980/kaspersky-lab-a-cybersecurity-leader-with-ties-to-russian-govt>

<sup>117</sup> Flintoff, 2015.

<sup>118</sup> Ians, "Kaspersky Lab joins Interpol-led cybercrime operation across Asian nations," *The Economic Times*, April 25, 2017, accessed May 17, 2017, <http://economictimes.indiatimes.com/tech/internet/kaspersky-lab-joins-interpol-led-cybercrime-operation-across-asean-nations/articleshow/58360723.cms>.

security companies also cooperate with other countries.<sup>119</sup> 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.<sup>120</sup> Programs like these create ground for greater international cooperation and information sharing in the future.

---

<sup>119</sup> Ians, 2017.

<sup>120</sup> David Shukman, "Open Sesame: Science Center Unveiled in Jordan," *BBC News: Science & Environment*, May 16, 2017, accessed May 17, 2017, <http://www.bbc.com/news/science-environment-39927836>.

## 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 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.

<b>Actors</b>	<p><i>Private</i></p> <ul style="list-style-type: none"> <li>- Researchers, journalists, non-governmental organizations (NGOs)</li> </ul>	<i>Public</i>
<b>Actions</b>	<ul style="list-style-type: none"> <li>- Investigates human rights abuses, lobbies governments, and promotes outreach campaigns<sup>121</sup></li> </ul>	
<b>Authority</b>	<ul style="list-style-type: none"> <li>- Reputational</li> </ul>	
<b>Structure</b>	<ul style="list-style-type: none"> <li>- An international secretariat body and international board provide general leadership</li> <li>- Regional sections exist in 70 countries around the world<sup>122</sup></li> </ul>	
<b>Norms</b>	<ul style="list-style-type: none"> <li>- Statute of Amnesty International (2005)</li> <li>- International Non-Governmental Organization (INGO) Accountability Charter (2006)</li> </ul>	
<b>Attribution</b>	<ul style="list-style-type: none"> <li>- Publicly publishes research on human rights violations</li> <li>- Organization abides by an open information policy</li> </ul>	
<b>Budget and Funding Source(s)</b>	<ul style="list-style-type: none"> <li>- \$250 million (2016)</li> <li>- Funded by independent donations<sup>123</sup></li> </ul>	
<b>Best Practices</b>	<ul style="list-style-type: none"> <li>- <b>Prominent regional divisions foster greater international cooperation</b></li> <li>- <b>High level of transparency</b></li> </ul>	

<sup>121</sup> "Who We Are," *Amnesty International*, accessed April 29, 2017, <https://www.amnesty.org/en/who-we-are/>.

<sup>122</sup> "Structure and People," *Amnesty International*, accessed May 1, 2017, <https://www.amnesty.org/en/about-us/how-were-run/structure-and-people/>.

<sup>123</sup> "2016 Global Financial Report," accessed April 29, 2017, <https://www.amnesty.org/en/2016-global-financial-report/>.

Actors	<i>Private</i> <ul style="list-style-type: none"> <li>- University of Toronto-based interdisciplinary research lab</li> </ul>	<i>Public</i>
<b>Actions</b>	<ul style="list-style-type: none"> <li>- Engages on the core issues of Internet openness and security from a human rights perspective<sup>124</sup></li> <li>- Reports are published publicly, sometimes with media<sup>125</sup></li> </ul>	
<b>Authority</b>	<ul style="list-style-type: none"> <li>- Reputational<sup>126</sup></li> </ul>	
<b>Structure</b>	<ul style="list-style-type: none"> <li>- A global research network<sup>127</sup></li> </ul>	
<b>Norms</b>	<ul style="list-style-type: none"> <li>- Procedural transparency<sup>128</sup></li> <li>- Diverse geographic representation<sup>129</sup></li> <li>- Academic peer-review<sup>130</sup></li> <li>- Open source sharing of information and technical tools<sup>131</sup></li> </ul>	
<b>Attribution</b>	<ul style="list-style-type: none"> <li>- Makes all findings public, often directly implicating actors<sup>132</sup></li> </ul>	
<b>Budget and Funding Source(s)</b>	<ul style="list-style-type: none"> <li>- Private foundations, institutes, and organizations<sup>133</sup></li> </ul>	
<b>Best Practices</b>	<ul style="list-style-type: none"> <li>- <b>Mixed method approach to investigation and analysis; combines technical and geopolitical expertise</b></li> <li>- <b>Geographic diversity, engages in capacity building with members from the Global South</b></li> <li>- <b>Stakeholder outreach via organizing and participating in global conferences</b></li> <li>- <b>Autonomy from government and commercial interests</b></li> </ul>	

<sup>124</sup> BPR Administration, “BPR Interview: Citizens Lab Director Ronald Deibert,” *Brown Political Review*, October 21, 2012, accessed June 5, 2017, <http://www.brownpoliticalreview.org/2012/10/interview-citizens-lab-director-ronald-deibert/>.

<sup>125</sup> See, for instance, Mattathias Schwartz, “Cyberwar For Sale,” *The New York Times Magazine*, January 4, 2017, accessed June 7, 2017, <https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html>.

<sup>126</sup> See, for instance, Anita Elash, “How The Citizen Lab polices the world’s digital spies,” *CS Monitor*, December 22, 2016, accessed June 7, 2017, <http://www.csmonitor.com/World/Passcode/2016/1222/How-The-Citizen-Lab-polices-the-world-s-digital-spies>.

<sup>127</sup> Ibid.

<sup>128</sup> Eva Galperin, Morgan Marquis-Borire, and John Scott-Railton, “Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns,” *Citizen Lab-EEF*, December 23, 2013, accessed June 7, 2017, <https://www.eff.org/document/quantum-surveillance-familiar-actors-and-possible-false-flags-syrian-malware-campaigns>.

<sup>129</sup> “About the Citizen Lab,” accessed June 5, 2017, <https://citizenlab.org/about/>; “Cyber Stewards,” accessed June 7, 2017, <https://cyberstewards.org/>; and “Open Net Initiative,” accessed June 7, 2017, <https://opennet.net/>.

<sup>130</sup> “Citizen Lab | Github,” accessed June 7, 2017, <https://github.com/citizenlab>.

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

<sup>132</sup> Ibid.

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

## Egmont Group of Financial Intelligence Units

Actors	<i>Private</i> <ul style="list-style-type: none"> <li>- Financial institutions and non-financial institutions</li> </ul>	<i>Public</i> <ul style="list-style-type: none"> <li>- Financial Intelligence Units (FIU)</li> </ul>
<b>Actions</b>	<ul style="list-style-type: none"> <li>- Submits cash-transaction and suspicious activity reports to the appropriate FIUs<sup>134</sup></li> </ul>	<ul style="list-style-type: none"> <li>- Different types of FIUs have different objectives</li> <li>- Some FIUs notify proper agencies to enforce laws, freezing and blocking suspicious transactions and accounts, and arrest suspects<sup>135</sup></li> </ul>
<b>Authority</b>	<ul style="list-style-type: none"> <li>- Corporate Executives and Boards of Directors</li> </ul>	<ul style="list-style-type: none"> <li>- Domestic law</li> <li>- United Nations (UN) Conventions<sup>136</sup></li> </ul>
<b>Structure</b>	<ul style="list-style-type: none"> <li>- Varies by institution</li> </ul>	<ul style="list-style-type: none"> <li>- Each FIU has its own complex structure, dense network of internal bodies, and process-specific groups<sup>137</sup></li> </ul>
<b>Norms</b>	<ul style="list-style-type: none"> <li>- Managerial discretion</li> <li>- Local and/or national law</li> <li>- 2003 Financial Action Task Force (FATF) recommendations based on Vienna and Palermo Conventions<sup>138</sup></li> </ul>	<ul style="list-style-type: none"> <li>- FATF recommendations<sup>139</sup></li> </ul>
<b>Attribution</b>	<ul style="list-style-type: none"> <li>- No attributive properties; works solely as an information-gathering organization</li> </ul>	<ul style="list-style-type: none"> <li>- Name organizations that fail to uphold reporting standards and laws<sup>140</sup></li> <li>- Attribution information is shared between FIUs through communiques, plenary meetings, and trainings<sup>141</sup></li> </ul>
<b>Budget and Funding Source(s)</b>	<ul style="list-style-type: none"> <li>- Budgets vary from institution to institution</li> <li>- Funds for each institution are acquired through debt and equity</li> </ul>	<ul style="list-style-type: none"> <li>- Budgets vary from nation to nation</li> <li>- Funding provided by national governments</li> <li>- United States FIU (FinCEN) has proposed budget of approximately \$155M in 2017<sup>142</sup></li> </ul>
<b>Best Practices</b>	<ul style="list-style-type: none"> <li>- <b>Suspicious Activity Reports function as preventative measures that can also provide information needed to launch criminal investigations</b></li> </ul>	<ul style="list-style-type: none"> <li>- <b>Process Improvement Groups promote information exchange and adherence to financial standards created by the Egmont Group</b></li> <li>- <b>Heavy emphasis on communication and training mechanisms ensure cooperation and cohesion</b></li> </ul>

<sup>134</sup> International Monetary Fund, and World Bank. "Financial Intelligence Units: An Overview," 2004. <https://www.imf.org/external/pubs/ft/FIU/fiu.pdf>.

<sup>135</sup> Ibid.

<sup>136</sup> "Money Laundering and the Financing of Terrorism - The Egmont Group." Accessed April 30, 2017. <https://egmontgroup.org/en/content/money-laundering-and-financing-terrorism>.

<sup>137</sup> "Structure and Organization of the Egmont Group of Financial Intelligence Units," The Egmont Group. Accessed April 3, 2017. <https://www.egmontgroup.org/en/content/structure-and-organization-egmont-group-financial-intelligence-units>.

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

<sup>139</sup> Financial Action Task Force. "INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION." FAFTA/OECD, 2013. [http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF\\_Recommendations.pdf](http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf).

<sup>140</sup> "News | FinCEN.gov." Accessed April 30, 2017. <https://www.fincen.gov/news-room/news>.

<sup>141</sup> "Public Statements and Communiques - The Egmont Group." Accessed April 3, 2017. <https://www.egmontgroup.org/en/document-library/9>.

<sup>142</sup> International Monetary Fund, and World Bank, 2004.

## European Financial Coalition Against Child Pornography (EFCACP)

<b>Actors</b>	<i>Private</i> - Banks, payment companies, Internet service providers	<i>Public</i> - Europol, European Union (EU)
<b>Actions</b>	- Cooperates with the EFCACP to design and launch initiatives to stop the sexual exploitation of children online - Works to prevent the transferring of funds for child pornography through credit cards and other online payment methods - ISPs work to implement a better system for detecting and blocking pornographic content <sup>143</sup>	- Fights sexual exploitation of children online by disrupting the economics of the illegal industry - Promotes awareness, cross-sector training sessions, and policy research and promotion <sup>144</sup>
<b>Authority</b>	- Reputational	- EU
<b>Structure</b>	- Partnerships are established on a voluntary basis - Representatives from private industry sit on the Steering Committee <sup>145</sup>	- Bureaucratic; one of many regional branches of the Financial Coalition Against Child Pornography - The EFCACP is chaired by Europol and led by a Steering Committee Functions as a branch of the European Cyber Centre at Europol
<b>Norms</b>	- UN Convention on the Rights of the Child - NGO/Industry best practices	- UN Convention on the Rights of the Child
<b>Attribution</b>	- No attributive properties	- No attributive properties, but shares information with other EU bodies
<b>Budget and Funding Source(s)</b>		- Part of Europol's \$114.6 million budget (2017) - Funding provided by EU member states <sup>146</sup>
<b>Best Practices</b>	- <b>Wide range of private actors from multiple fields have a seat at the table and are involved in the organization's structure and agenda</b> - <b>The private sector is directly responsible for carrying out initiatives to stop any financial gain related to child sexual exploitation</b>	- <b>Prominent regional divisions foster greater international cooperation</b>

<sup>143</sup> "Commercial Child Pornography: A Brief Snapshot of the Financial Coalition Against Child Pornography," National Center for Missing and Exploited Children, (2016), [http://www.missingkids.com/en\\_US/documents/Commercial\\_child\\_pornography\\_-\\_A\\_brief\\_snapshot\\_of\\_the\\_FCACP\\_2016.pdf](http://www.missingkids.com/en_US/documents/Commercial_child_pornography_-_A_brief_snapshot_of_the_FCACP_2016.pdf).

<sup>144</sup> "News from the EFC: The Past, The Present, The Future," accessed April 28, 2017, <http://us11.campaign-archive1.com/?u=a39d608c8102dd5c712efbc48&id=d1ce5b24df>.

<sup>145</sup> "EFC Members," *European Financial Coalition against Commercial Sexual Exploitation of Children Online*, n.d., [http://www.europeanfinancialcoalition.eu/efc\\_members.php](http://www.europeanfinancialcoalition.eu/efc_members.php).

<sup>146</sup> "Statement of Revenue and Expenditure of the European Police Office for the Financial Year 2017" (Office Journal of the European Union, n.d.).

## The Financial Industry Regulatory Authority (FINRA)

<b>Actors</b>	<i>Private</i> - Self-regulating private corporation	<i>Public</i> - Securities Exchange Council (SEC), Justice Department, and the Federal Bureau of Investigation (FBI)
<b>Actions</b>	- Monitors US equities, shares information with authorities - Protects investors by upholding the integrity of US financial market, and levies fines against brokers <sup>147</sup>	- Use FINRA's information to build evidence for the prosecution of securities fraud
<b>Authority</b>	- Performs regulatory oversight of securities firms selling to public investors through contracts with stock exchanges <sup>148</sup>	- The Securities and Exchange Act; SEC's extraterritorial exercise of its jurisdiction
<b>Structure</b>	- 3,400 employees based in Washington, D.C. and New York City with 20 regional offices <sup>149</sup>	- Bureaucratic agencies within the federal government
<b>Norms</b>	- Complies with the Federal Reserve and laws regulating data and information privacy - Uses an arbitration forum - Board members are publicly elected <sup>150</sup>	- Press briefings, disclosure, laws regulating evidence collection and prosecution <sup>151</sup>
<b>Attribution</b>	- Discloses information publicly in reports and with law enforcement <sup>152</sup>	- Yes, and prosecution <sup>153</sup>
<b>Budget and Funding Source(s)</b>	- \$878.6 million (2012) - Funded by the businesses it regulates <sup>154</sup>	- Budget is provided by the US government
<b>Best Practices</b>	- <b>Public disclosure</b> - <b>Use of technology to detect fraud, centralized database</b> <sup>155</sup> - <b>Collaboration with authorities</b>	- <b>Strong norms and laws guide investigations</b> - <b>Public disclosure</b> - <b>Public-private cooperation</b>

<sup>147</sup> "About FINRA," finra.org, accessed May 1, 2017. <https://www.finra.org/about>; Carrie Johnson, "SEC Approves One Watchdog For Brokers Big and Small," *The Washington Post*, July 27, 2007, Page D02., accessed May 2, 2017, [http://www.washingtonpost.com/wp-dyn/content/article/2007/07/27/AR2007072700108\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2007/07/27/AR2007072700108_pf.html).

<sup>148</sup> Ibid., 8

<sup>149</sup> Ibid., 72.

<sup>150</sup> Ibid., 72; "Board of Governors," finra.org. Accessed 2 May 2017. <https://www.finra.org/about/finra-board-governors>; An Outline of the FINRA Arbitration Process For Customer-Broker Disputes - Smiley Bishop & Porter LLP," April 20, 2011, accessed May 2 2017, <http://www.sbppllaw.com/2011/04/an-outline-of-the-finra-arbitration-process-for-customer-broker-disputes/>.

<sup>151</sup> Michael Feldberg, "U.S. Insider Trading Enforcement Goes Global," *Allen & Overy LLP*, May 2, 2013.

<sup>152</sup> For an analysis of FINRA's annual letter see, "FINRA 2014 exams: Variable annuities," *PwC Financial Services Regulatory Practice*, January, 2015, accessed May 2, 2017, [http://www.pwc.com/en\\_US/us/financial-services/regulatory-services/publications/assets/finra-exams-variable-annuities.pdf](http://www.pwc.com/en_US/us/financial-services/regulatory-services/publications/assets/finra-exams-variable-annuities.pdf); Azam Ahmed, "Amid Insider Trading Inquiry, Tiger Asia Calls It Quits," *New York Times*, August 14, 2012, accessed May 1, 2017, [https://dealbook.nytimes.com/2012/08/14/amid-insider-trading-inquiry-tiger-asia-calls-it-quits/?\\_r=0](https://dealbook.nytimes.com/2012/08/14/amid-insider-trading-inquiry-tiger-asia-calls-it-quits/?_r=0).

<sup>153</sup> SEC Press Release 2012-264, *Hedge Fund Manager to Pay \$44 Million for Illegal Trading in Chinese Bank Stocks*, December 12, 2012, accessed May 1, 2017, <https://www.sec.gov/news/press-release/2012-2012-264.htm>.

<sup>154</sup> Ibid., 8

<sup>155</sup> See for instance, "Technology FINRA," finra.org, accessed May 1 2017, <https://www.finra.org/about/technology>; "Central Registration Depository (Web CRD)," finra.org, accessed May 2, 2017, <http://www.finra.org/industry/compliance/registration/crd/>.

<b>Actors</b>	<i>Private</i> - Members and volunteers	<i>Public</i>
<b>Actions</b>	- Research and lobbying on cases of environmental destruction	
<b>Authority</b>	- Reputational - Consultative status with UN Economic and Social Council	
<b>Structure</b>	- 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 <sup>156</sup>	
<b>Norms</b>	- Responsibility, nonviolence, independence and neutrality, as listed in Greenpeace's core values <sup>157</sup>	
<b>Attribution</b>	- 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 <sup>158</sup>	
<b>Budget and Funding Source(s)</b>	- \$349.8 million (2015), collected from donations of 2.9 million members <sup>159</sup>	
<b>Best Practices</b>	- <b>Independence from public sector</b> - <b>Strong reputational authority</b>	

<sup>156</sup> "Greenpeace structure and organization." Greenpeace International. 2017. accessed April 30, 2017. <http://www.greenpeace.org/international/en/about/how-is-greenpeace-structured/>.

<sup>157</sup> "Our core values." Greenpeace International, accessed April 30, 2017. <http://www.greenpeace.org/international/en/about/our-core-values/>.

<sup>158</sup> "Our Inflatables." Greenpeace International, accessed April 30, 2017. <http://www.greenpeace.org/international/en/about/ships/our-inflatables/>.

<sup>159</sup> *Greenpeace International Annual Report 2015. Report. 2015*, accessed, April 30, 2017, <http://www.greenpeace.org/international/Global/international/publications/greenpeace/2016/2015-Annual-Report-Web.pdf>.

## International Atomic Energy Agency (IAEA)

<b>Actors</b>	<i>Private</i> - Atomic energy experts and employees	<i>Public</i> - 168 member states
<b>Actions</b>	- Set nuclear safety standards - Help member states meet safety standards - Verify compliance with international safeguards <sup>160</sup>	- Comply with Safeguards/Additional Protocol - Declare all nuclear facilities and materials, aid other member states <sup>161</sup>
<b>Authority</b>	- UN	- Individual member states report to the Board of Governors, General Conference
<b>Structure</b>	- The Secretariat consists of five offices and six departments staffed by experts from the private sector - Board of Governors consisting of representatives from 22 member states; each state must be elected by the General Conference - The General Conference contains delegates of all 168 member states that meet once a year to approve actions and budgets	- National energy agencies, such as the US Nuclear Regulatory Commission and the Department of Energy, work alongside IAEA offices and departments <sup>162</sup>
<b>Norms</b>	- Based around the policy of nuclear non-proliferation	- Each state is bound to the Safeguards/Additional Protocol
<b>Attribution</b>	- Attribute safety violations through materials and facilities inspections <sup>163</sup>	- States can attribute domestic problems by conducting self-evaluation and peer-review inspections before official IAEA inspections
<b>Budget and Funding Source(s)</b>	- \$391.5 million (2016) <sup>164</sup> - Funded by member states and other donations	- Each member state has its own energy budget
<b>Best Practices</b>	- <b>Political neutrality</b> - <b>Collaboration within the private sector</b> - <b>Different branches of the organization serve as a form of checks and balances</b>	- <b>Emphasis on cooperation between government agencies</b> - <b>Provide a framework for self-assessment</b> - <b>Have formal agreements, such as the founding statute and Safeguard, that act as the basis for IAEA operation</b>

<sup>160</sup> "International Atomic Energy Agency (IAEA) IAEA Home," iaea.org, accessed April 30, 2017, <https://www.iaea.org/OurWork/>.

<sup>161</sup> "IAEA Safeguards Overview," iaea.org, accessed April 30, 2017, <https://www.iaea.org/publications/factsheets/iaea-safeguards-overview>.

<sup>162</sup> "Member States' Competent Authorities," iaea.org, accessed April 30, 2017, <http://www-ns.iaea.org/tech-areas/emergency/member-states-competent-authorities.asp?s=1>.

<sup>163</sup> "IAEA Safety Standards," iaea.org, accessed April 30, 2017, <http://www-ns.iaea.org/standards/>.

<sup>164</sup> "The Agency's Programme and Budget 2016 –2017," Rep. N.p.: IAEA, 2015., accessed April 30, 2017, [https://www.iaea.org/About/Policy/GC/GC59/GC59Documents/English/gc59-2\\_en.pdf](https://www.iaea.org/About/Policy/GC/GC59/GC59Documents/English/gc59-2_en.pdf).

## International Civil Aviation Organization (ICAO)

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

<sup>165</sup> "About." Join Our Project-Based Initiatives," icao.int, accessed April 30, 2017, <http://www.icao.int/about-icao/partnerships/Pages/default.aspx>.

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

<sup>167</sup> "Making an ICAO Standard," icao.int, accessed April 30, 2017, <http://www.icao.int/safety/airnavigation/Pages/standard.aspx#4>.

<sup>168</sup> "About ICAO," icao.int, accessed April 30, 2017, <http://www.icao.int/about-icao/Pages/default.aspx>.

<sup>169</sup> "ICAO: Frequently Asked Questions," icao.org, accessed April 30, 2017, <http://www.icao.int/about-icao/FAQ/Pages/icao-frequently-asked-questions-faq-2.aspx>.

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

<sup>171</sup> "Budget of the Organization 2017-2018-2019," icao.int, accessed April 29, 2017, [http://www.icao.int/publications/Documents/10074\\_en.pdf](http://www.icao.int/publications/Documents/10074_en.pdf).

<sup>172</sup> "ICAO's Response to Global Challenges," *Act Global*, 2009, accessed April 29, 2017, <http://www.icao.int/Newsroom/News%20Doc/copenhaguen-complete134ec9.pdf>.

## International Labor Organization (ILO)

<b>Actors</b>	<i>Private</i>	<i>Public</i> - 187 member states
<b>Actions</b>		- Represents employment and workers, registers complaints, sets global labor standards, <sup>173</sup> and investigates violations of workers' rights <sup>174</sup>
<b>Authority</b>		- UN Charter - ILO Conventions
<b>Structure</b>		- 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
<b>Norms</b>		- Routine monitoring, free and open debate, <sup>175</sup> declaration of fundamental of principles, <sup>176</sup> equal geographic representation, and a tripartite government structure
<b>Attribution</b>		- Release findings after a process of evidence collection, standardization, assessment of legal burden, and a review process <sup>177</sup>
<b>Budget and Funding Source(s)</b>		- \$225.7 million (2015) - Funded by contributions from member states and donations <sup>178</sup>
<b>Best Practices</b>		- <b>An efficient system to launch complaints and establish transparency reports</b>

<sup>173</sup> "Mission and Impact of the ILO," ilo.org, accessed May 3, 2017, <http://ilo.org/global/about-the-ilo/mission-and-objectives/lang--en/index.htm>.

<sup>174</sup> "Government's Recent Labour Interventions Highly Unusual, Experts Say," *CBC News*, accessed May 3, 2017, <http://www.cbc.ca/news/canada/government-s-recent-labour-interventions-highly-unusual-experts-say-1.977658>.

<sup>175</sup> "International Labour Conference," ilo.org, accessed May 3, 2017, <http://ilo.org/global/about-the-ilo/how-the-ilo-works/international-labour-conference/lang--en/index.htm>.

<sup>176</sup> "ILO Declaration on Fundamental Principles and Rights at Work (DECLARATION)," accessed May 3, 2017, <http://www.ilo.org/declaration/lang--en/index.htm>.

<sup>177</sup> On how the ILO acts as a vehicle to investigate noncompliance see: Berik, Günseli and Yana Van der Meulen Rodgers, "Options for enforcing labour standards: Lessons from Bangladesh and Cambodia," *Journal of International Development* 22 (2008): 56-85, accessed April 30, 2017, [www.interscience.wiley.com](http://www.interscience.wiley.com).

<sup>178</sup> "Programme and Budget," ilo.org, accessed May 3, 2017, <http://embargo.ilo.org/global/about-the-ilo/how-the-ilo-works/programme-and-budget/lang--en/index.htm>.

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

<b>Actors</b>	<i>Private</i> - Companies in the defense industry, such as Siemens, Threod Systems, Cyber Test Systems, and more	<i>Public</i> - NATO member states and cooperating non-member states
<b>Actions</b>		- Promote cooperative cyber defense, establish cyberspace norms, and confidence-building measures <sup>179</sup>
<b>Authority</b>		- NATO
<b>Structure</b>		- International steering committee consisting of center’s sponsoring nations - The CCDCOE is not part of NATO’s military command or force structure, and is made up of military, government, and defense industry professionals - Center consists of researchers, analysts, trainers, educators <sup>180</sup>
<b>Norms</b>		- Tallinn Manual <sup>181</sup>
<b>Attribution</b>		- Attributes cyberattacks in published articles, but is mostly focused on building cyberinfrastructure, and cyberdefense capabilities <sup>182 183</sup>
<b>Budget and Funding Source(s)</b>		- Funded by NATO and Non-NATO members
<b>Best Practices</b>		- <b>Multinational information sharing</b> - <b>Promoting collective cyberdefense</b> - <b>Accumulating, creating, and disseminating international cyberexpertise</b>

NATO, “About Cyber Defence Centre | CCDCOE,” *NATO Cooperative Cyber Defence Centre of Excellence*, accessed April 30, 2017, <https://ccdcoe.org/about-us.html>.

Structure | CCDCOE,” accessed May 4, 2017, <https://ccdcoe.org/structure-0.html>.

<sup>181</sup> Tallinn Manual Process | CCDCOE,” accessed May 4, 2017, <https://ccdcoe.org/tallinn-manual.html>.

<sup>182</sup> Jeffrey Carr, “Responsible Attribution: A Prerequisite For Accountability,” *NATO CCD COE*, The Tallinn Papers, no. No.6 (2014): 1–8.

son 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)

<b>Actors</b>	<i>Private</i> - Independent scientists and NGOs	<i>Public</i> - 192 member countries
<b>Actions</b>	- Oversee outreach and training programs with chemical industry - Collaborates to review processes of verification and chemical weapons disarmament	- Carries out verification measures, facilitates chemical weapons inspections, and negotiates agreements with state parties <sup>184</sup>
<b>Authority</b>	- Reputational	- UN
<b>Structure</b>	- Independent scientists sit on the Scientific Advisory Board - INGOs like the International Union of Pure and Applied Chemistry provide a consultative and outreach role - Private companies can sign a Memorandum of Understanding with the OPCW to solidify cooperation <sup>185</sup>	- Led by a Director-General - Equitable geographic distribution in decision-making bodies
<b>Norms</b>	- OPCW and International Union of Pure and Applied Chemistry code of ethical principles of chemistry <sup>186</sup>	- 1997 Convention on Chemical Weapons
<b>Attribution</b>	- No public attributive properties; private actors do not release information about ongoing investigations	- No public attributive properties; do not release information about ongoing investigations
<b>Budget and Funding Source(s)</b>		- \$95 Million (2012) - Funded by member states, whose contribution is calculated based on the UN scale of assessment <sup>187</sup>
<b>Best Practices</b>	- <b>Involves chemical industry in outreach training programs and norms building</b> - <b>Scientists actively participate in advising and facilitating disarmament on a rotational and elected basis</b>	- <b>Equitable geographic distribution among all bodies of the organization</b> - <b>On-the-ground inspections and fact-finding missions give the OPCW a tangible presence in member countries</b> - <b>Broad international treaty gives the organization a clear legal mandate and set of duties</b>

<sup>184</sup> "OPCW Mission Statement," *Organization for the Prohibition of Chemical Weapons*, n.d., accessed April 30, 2017, <https://www.opcw.org/about-opcw/mission/>.

<sup>185</sup> "IUPAC and the Organization for the Prohibition of Chemical Weapons Take Partnership to New Level| International Union of Pure and Applied Chemistry," *IUPAC, International Union of Pure and Applied Chemistry*, December 1, 2016, accessed April 30, 2017, <https://iupac.org/iupac-opcw-take-partnership-new-level/>.

<sup>186</sup> "International Union of Pure & Applied Chemistry," *IUPAC, International Union of Pure and Applied Chemistry*, accessed April 28, 2017, <https://iupac.org/who-we-are/>.

<sup>187</sup> "Organization for the Prohibition of Chemical Weapons," *NIT: Building a Safer World*, April 28, 2017, accessed April 30, 2017, <http://www.nti.org/learn/treaties-and-regimes/organization-for-the-prohibition-of-chemical-weapons/>.

## United Nations Al-Qaida Sanctions Committee

<b>Actors</b>	<i>Private</i> - Monitoring Team comprised of independent researchers and experts	<i>Public</i> - UN member states
<b>Actions</b>	- Assists committee and UN member states in identifying and gathering information on sanctioned individuals and monitors cases of state non-compliance with sanction operations <sup>188</sup>	- 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 <sup>189</sup>
<b>Authority</b>	- UN	- UN
<b>Structure</b>	- Independent branch of the Sanctions Committee	- Decision-making done through member state consensus - All members of the UNSC are represented <sup>190</sup>
<b>Norms</b>	- United Nations Security Council (UNSC) Resolution 1267	- UNSC Resolution 1267
<b>Attribution</b>	- Presents findings to UNSC/UN Sanctions Committee	- Publicly discloses the sanctions list
<b>Budget and Funding Source(s)</b>	- Part of Committee budget	- \$39.6 million (2015) for all Sanctions Committees - Funded by contributions from UN member states <sup>191</sup>
<b>Best Practices</b>	- <b>Cooperate directly with member states in implementation and information-gathering</b> - <b>Conducts independent assessments and ensure compliance and state accountability</b> <sup>192</sup>	- <b>Ombudsperson helps with legal credibility and internal accountability</b> <sup>193</sup> - <b>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</b>

<sup>188</sup> "Resolution 2253 (2015)" *United Nations Security Council*, December 17, 2015, accessed April 29, 2017, [http://www.un.org/en/ga/search/view\\_doc.asp?symbol=S/RES/2253\(2015\)](http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2253(2015)).

<sup>189</sup> "Guidelines of the Committee for the Conduct of Its Work" *United Nations Security Council*, December 23, 2016, accessed April 25, 2017,

[https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/guidelines\\_of\\_the\\_committee\\_for\\_the\\_conduct\\_of\\_its\\_work.pdf](https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/guidelines_of_the_committee_for_the_conduct_of_its_work.pdf).

<sup>190</sup> *Ibid.*, 55

<sup>191</sup> "General Assembly, on Fifth Committee's Recommendation, Adopts Raft of Texts on 2014-2015 Biennium Budget Appropriations, Common System, Peacekeeping," *United Nations*, accessed April 27, 2017,

<https://www.un.org/press/en/2014/ga11608.doc.htm>.

<sup>192</sup> "Work and Mandate," *United Nations Security Council Subsidiary Organs*, accessed April 29, 2017, <https://www.un.org/sc/suborg/en/sanctions/1267/monitoring-team/work-and-mandate>.

<sup>193</sup> "Procedure," *Office of the Ombudsperson of the Security Council's 1267 Committee*, accessed April 29, 2017, <https://www.un.org/sc/suborg/en/ombudsperson/procedure>.

## United Nations Sanctions Committee on North Korea

<b>Actors</b>	<p><i>Private</i></p> <ul style="list-style-type: none"> <li>- Panel of Experts composed of professionals from nuclear, weapon of mass destruction, import/export controls, and financial industries<sup>194</sup></li> </ul>	<p><i>Public</i></p> <ul style="list-style-type: none"> <li>- UN member states</li> </ul>
<b>Actions</b>	<ul style="list-style-type: none"> <li>- Helps the Sanctions Committee gather evidence, analyze information, and assess the implementation of sanctions</li> <li>- Advises Sanctions Committee as they decide how to utilize sanctions<sup>195</sup></li> </ul>	<ul style="list-style-type: none"> <li>- Imposes constraints on diplomats, inspects suspicious cargo, and expands a blacklist of items North Korea is prohibited from importing<sup>196</sup></li> </ul>
<b>Authority</b>	<ul style="list-style-type: none"> <li>- UN, US law</li> <li>- Reputational</li> </ul>	<ul style="list-style-type: none"> <li>- UN</li> </ul>
<b>Structure</b>	<ul style="list-style-type: none"> <li>- Panel acts under the direction of the Sanctions Committee</li> <li>- Panelists are appointed by UN Secretary General<sup>197</sup></li> </ul>	<ul style="list-style-type: none"> <li>- Centralized bureaucracy with decision-making done through member state consensus<sup>198</sup></li> <li>- All members of the UNSC are represented</li> </ul>
<b>Norms</b>	<ul style="list-style-type: none"> <li>- Purely informational, advisory role with no decision-making capacities<sup>199</sup></li> </ul>	<ul style="list-style-type: none"> <li>- A system of routine monitoring, narrow mandate, impromptu meetings, a declaration of fundamental principles,<sup>200</sup> and geographic representation<sup>201</sup> govern UNSC Resolutions relating to North Korea</li> </ul>
<b>Attribution</b>	<ul style="list-style-type: none"> <li>- Publicly publish reports on findings on an annual basis<sup>202</sup></li> </ul>	<ul style="list-style-type: none"> <li>- Sanctions list is public, naming specific industries</li> </ul>
<b>Budget and Funding Source(s)</b>	<ul style="list-style-type: none"> <li>- Funded by UN Sanctions Committee, UN member states</li> </ul>	<ul style="list-style-type: none"> <li>- Part of the UN budget for the Security Council and Sanctions Committees<sup>203</sup></li> <li>- Funded by contributions from UN member states</li> </ul>
<b>Best Practices</b>	<ul style="list-style-type: none"> <li>- <b>Integration of private sector experts into the decisions of a large, inter-governmental body</b></li> </ul>	<ul style="list-style-type: none"> <li>- <b>Useful model for many countries that agree upon attribution to coordinate and assess fault and compliance</b></li> </ul>

<sup>194</sup> "Work and Mandate." *Security Council Committee Established Pursuant to Resolution 1718 (2006)*, n.d. [https://www.un.org/sc/suborg/en/sanctions/1718/panel\\_experts/work\\_mandate](https://www.un.org/sc/suborg/en/sanctions/1718/panel_experts/work_mandate).

<sup>195</sup> Ibid.

<sup>196</sup> "United Nations Resolution 1718," *globalpolicy.org*, accessed May 3, 2017, <https://www.globalpolicy.org/images/pdfs/1014reso1718.pdf>.

<sup>197</sup> Ibid.

<sup>198</sup> "Functions and Powers of the United Nations Security Council," *un.org*, accessed May 3, 2017, <http://www.un.org/en/sc/about/functions.shtml>.

<sup>199</sup> Mary Beth Niktin, Mark E. Manyin, Emma Chanlett-Avery, and Dick K. Nanto. "North Korea's Second Nuclear Test: Implications of U.N. Security Council Resolution 1874." Congressional Research Service, April 15, 2010. <https://fas.org/sgp/crs/nuke/R40684.pdf>.

<sup>200</sup> "Chapter I | United Nations," *un.org*, accessed May 3, 2017, <http://www.un.org/en/sections/un-charter/chapter-i/index.html>.

<sup>201</sup> "Members of the United Nations Security Council," *un.org*, accessed May 3, 2017, <http://www.un.org/en/sc/members/>.

<sup>202</sup> "Reports," n.d. [https://www.un.org/sc/suborg/en/sanctions/1718/panel\\_experts/reports](https://www.un.org/sc/suborg/en/sanctions/1718/panel_experts/reports).

<sup>203</sup> Susan Kurtas, "Research Guides: UN Documentation: Security Council: Introduction," *Research.un.org*, accessed May 3, 2017. <http://research.un.org/en/docs/sc/introduction>.

## World Trade Organization (WTO) GATT Article XX

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

<sup>204</sup> Thomas H. Oatley, "Debates in International Political Economy," (Boston: Longman, 2012.) Print.

<sup>205</sup> "WTO Trade and Environment," *WTO.org*, accessed April 30, 2017, [https://www.wto.org/english/tratop\\_e/envir\\_e/envt\\_rules\\_exceptions\\_e.htm](https://www.wto.org/english/tratop_e/envir_e/envt_rules_exceptions_e.htm).

<sup>206</sup> "WTO Understanding the WTO - A unique contribution," *WTO.org*, accessed April 30, 2017, [https://www.wto.org/english/thewto\\_e/whatis\\_e/tif\\_e/disp1\\_e.htm](https://www.wto.org/english/thewto_e/whatis_e/tif_e/disp1_e.htm).

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

<sup>208</sup> "Annual Report 2016 - Secretariat and Budget," *WTO Secretariat*, 2016, accessed April 29, 2017. [https://www.wto.org/english/res\\_e/booksp\\_e/anrep\\_e/anrep16\\_chap9\\_e.pdf](https://www.wto.org/english/res_e/booksp_e/anrep_e/anrep16_chap9_e.pdf).

<sup>209</sup> "WTO Budget for the year 2015," *WTO.org*, accessed April 29, 2017, [https://www.wto.org/english/thewto\\_e/secret\\_e/budget\\_e.htm](https://www.wto.org/english/thewto_e/secret_e/budget_e.htm).

<sup>210</sup> "Work and Mandate," *United Nations Security Council Subsidiary Organs*, accessed April 29, 2017, <https://www.un.org/sc/suborg/en/sanctions/1267/monitoring-team/work-and-mandate>.

## 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)

<b>Actors</b>	<i>Private</i> - Media, academia, independent researchers <sup>211</sup>	<i>Public</i> - South Korean Government, technical and forensic experts in the Joint Investigation Group <sup>212</sup>
<b>Actions</b>	- Test and verify the JIG's report	- Determine the cause of Cheonan's sinking and deescalate tensions with North Korea <sup>213</sup>
<b>Authority</b>	- Credibility of individual organizations	- Experts credentials, government
<b>Structure</b>	- 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 - The JIG was divided into four departments: forensic science, explosive pattern analysis, hull structure, and data analysis <sup>214</sup>	- State-integrated, non-bureaucratic
<b>Norms</b>	- Peer-review, high-degree of transparency	
<b>Attribution</b>	- Evidence analysis and attribution judgment <sup>215</sup>	- Published an attribution report detailing evidence collection, evidence standard and analysis, and made final judgement in report <sup>216</sup>
<b>Budget and Funding Source(s)</b>		- Funded by South Korean government
<b>Best Practices</b>	- <b>Decentralized peer-review</b> - <b>Accessibility, low-barrier to entry</b>	- <b>Objective reading of evidence, default to neutrality</b> - <b>Quick investigation</b> - <b>Body composed of forensic and technical experts</b>

<sup>211</sup> See for instance, "How Did N. Korea Sink The Cheonan?" *Chosun Ilbo*, May 21, 2010, accessed May 1, 2017, [http://english.chosun.com/site/data/html\\_dir/2010/05/21/2010052100698.html](http://english.chosun.com/site/data/html_dir/2010/05/21/2010052100698.html); Yoichi Shimatsu, "Did an American Mine Sink South Korean Ship?" *New America Media*, May 27, 2010, accessed May 1, 2017, <http://newamericamedia.org/2010/05/did-an-american-mine-sink-the-south-korean-ship.php>; "Russian Navy Expert Team's analysis on the Cheonan incident," *The Hankyoreh*, July 27, 2010, accessed May 1, 2017, [http://english.hani.co.kr/arti/english\\_edition/e\\_northkorea/432230.html](http://english.hani.co.kr/arti/english_edition/e_northkorea/432230.html); Kim Myong Chol, "Pyongyang sees US role in Cheonan sinking," *Asia Times Online*, May 5, 2010, accessed April 29, 2017, <http://www.atimes.com/atimes/Korea/LE05Dg01.html>.

<sup>212</sup> "Investigation Result on the Sinking of ROKS Cheonan – report statement," Ministry of National Defense R.O.K., May 20, 2010. News item No 592., accessed May 1, 2017, <http://www.mnd.go.kr/webmodule/htsboard/template/read/engbdread.jsp?typeID=16&boardid=88&seqno=871&c=TITLE&t=&pagenum=3&tableName=ENGBASIC&pc=undefined&dc=&wc=&lu=&vu=&iu=&du=&st=>.

<sup>213</sup> Peter Foster and Malcolm Moore, "North Korea threatens 'all-out war' over warship sinking report," *The Telegraph*, May 20, 2010, accessed May 1, 2017, <http://www.telegraph.co.uk/news/worldnews/asia/northkorea/7745370/North-Korea-threatens-all-out-war-over-warship-sinking-report.html>.

<sup>214</sup> "Results Confirm North Korea Sank Cheonan," *Daily NK*, May 20, 2010, accessed May 1, 2017 <http://www.dailynk.com/english/read.php?catald=nk00100&num=6392>.

<sup>215</sup> "Cheonan sinking: top ten conspiracy theories," *The Daily Telegraph*, June 4, 2010, accessed May 1, 2017, <http://blogs.telegraph.co.uk/news/peterfoster/100042229/cheonan-sinking-top-ten-conspiracy-theories/>.

<sup>216</sup> Editorial, "The Sinking of the Cheonan," *New York Times*, May 20, 2010, accessed May 1, 2017, <http://www.nytimes.com/2010/05/21/opinion/21fri2.html>.

## Democratic National Committee (DNC) Email Leak Investigation

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

<sup>217</sup> Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times*, December 13, 2016, accessed April 25, 2017, [https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?\\_r=0](https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0).

<sup>218</sup> Fire Eye, "APT 28: A Window Into Russia's Cyber Espionage Operations?," Intelligence Report, (October 2014).

<sup>219</sup> *Ibid.*, 79

<sup>220</sup> "10 Top Cybersecurity Companies," accessed May 2, 2017, <http://investingnews.com/daily/tech-investing/cybersecurity-investing/top-cyber-security-companies/>.

<sup>221</sup> Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," *CROWDSTRIKE BLOG*, June 15, 2016, accessed April 29, 2017, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

<sup>222</sup> Fire Eye, "APT 28: At the Center of the Storm, Russia Strategically Evolves Its Cyber Operations," Intelligence Report, (January 2017).

<sup>223</sup> Federal Bureau of Investigation and U.S. Department of Homeland Security, "GRIZZLY STEPPE Russian Malicious Cyber Activity," Joint Analysis U.S. Government Report, (December 29, 2016).

<sup>224</sup> Office of the Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," U.S. Government, National Intelligence Council, (January 6, 2017).

## Google's Operation Aurora

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

<sup>225</sup> Kenneth Corbin, "'Aurora' Cyber Attackers Were Really Running Counter-Intelligence," *CIO.com*, April 22, 2013, accessed April 29, 2017, <http://www.cio.com/article/2386547/government/-aurora--cyber-attackers-were-really-running-counter-intelligence.html>; Michael Joseph Gross, "Enter the Cyber-Dragon," *VANITY FAIR*, September, 2011, at 222, accessed April 29, 2017, <http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109>.

<sup>226</sup> Shane Harris, "Google's Secret NSA Alliance: The terrifying deals between Silicon Valley and the Security State," *Salon*, November 16, 2014, accessed April 29, 2017, [http://www.salon.com/2014/11/16/googles\\_secret\\_nsa\\_alliance\\_the\\_terrifying\\_deals\\_between\\_silicon\\_valley\\_and\\_the\\_security\\_state](http://www.salon.com/2014/11/16/googles_secret_nsa_alliance_the_terrifying_deals_between_silicon_valley_and_the_security_state).

<sup>227</sup> Kim Zetter, "'Google' Hackers Had Ability to Alter Source Code," *Wired*, March 3, 2010, accessed April 27, 2017, <https://www.wired.com/2010/03/source-code-hacks>.

<sup>228</sup> "Best Practices for Victim Response and Reporting of Cyber Incidents," Cybersecurity Unit, Computer Crime & Intellectual Property Section, U.S. Department of Justice, April 29, 2015, accessed April 27, 2017, [https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal\\_division\\_guidance\\_on\\_best\\_practices\\_for\\_victim\\_response\\_and\\_reporting\\_cyber\\_incidents.pdf](https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf).

<sup>229</sup> *Ibid.*, 64

<sup>230</sup> Shane Huang, "Proposing a Self-Help Privilege for Victims of Cyber Attacks." *George Washington Law Review* 82 (2014): 1229-858.; 18 U.S.C. § 1030(a)(2) (2012).

<sup>231</sup> David Drummond, "A New Approach to China," *Google Official Blog*, January 12, 2010, accessed April 25, 2017, <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>.

<sup>232</sup> Hillary Rodham Clinton, U.S. Sec of State, Statement on Google Operations in China, January 12, 2010, accessed April 29, 2017, <https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135105.htm>.

<sup>233</sup> "DNI Releases Budget Figure for 2013 National Intelligence Program," Office of the Director of National Intelligence, October 30, 2013, accessed May 2, 2017, <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/957-dni-releases-budget-figure-for-2013-national-intelligence-program>.

<sup>234</sup> John Markoff, "Hackers Said to Breach Google Password System," *New York Times*, April 20, 2010, at A1., accessed April 29, 2017, <http://www.nytimes.com/2010/04/20/technology/20google.html>.

## Intermediate-Range Nuclear Force (INF) Treaty Investigative Process

<b>Actors</b>	<i>Private</i>	<i>Public</i> <ul style="list-style-type: none"> <li>- US Bureau of Arms Control, Verification and Compliance (AVC)</li> <li>- US and Russian governments, inter-governmental organizations that verify adherence to INF Treaty</li> </ul>
<b>Actions</b>		<ul style="list-style-type: none"> <li>- Conduct on-site inspections and verifications,<sup>235</sup> inter-state information exchange,<sup>236</sup> reconnaissance and data analyses<sup>237</sup></li> </ul>
<b>Authority</b>		<ul style="list-style-type: none"> <li>- US Department of State</li> </ul>
<b>Structure</b>		<ul style="list-style-type: none"> <li>- Centralized bureaucracy, government-to-government discussions and negotiations</li> </ul>
<b>Norms</b>		<ul style="list-style-type: none"> <li>- INF Treaty provisioned protocols<sup>238</sup></li> </ul>
<b>Attribution</b>		<ul style="list-style-type: none"> <li>- Both nations have attributed treaty violations to the other nation<sup>239</sup></li> </ul>
<b>Budget and Funding Source(s)</b>		<ul style="list-style-type: none"> <li>- \$32 million (2017) for compliance<sup>240</sup></li> <li>- Funded by the US Department of State</li> </ul>
<b>Best Practices</b>		<ul style="list-style-type: none"> <li>- <b>Information exchange between nations</b></li> <li>- <b>Process builds confidence between nations</b></li> <li>- <b>Strong definitions section in the INF Treaty</b></li> <li>- <b>Useful dispute resolution mechanism</b></li> </ul>

<sup>235</sup> Amy F. Woolf, Monitoring and Verification in Arms Control, *Congressional Research Service*, December 23, 2011, accessed May 2, 2017, <https://fas.org/sgp/crs/nuke/R41201.pdf>

<sup>236</sup> Ibid.

<sup>237</sup> Ibid.

<sup>238</sup> U.S. Department of State, "Treaty Between the United States Of America And The Union Of Soviet Socialist Republics on The Elimination of Their Intermediate-Range and Shorter-Range Missiles (INF Treaty)", accessed May 1, 2017, <https://www.state.gov/t/avc/trty/102360.htm>

<sup>239</sup> U.S. Department of State, "Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments," unclassified, July 2014, accessed May 1, 2017, <https://www.state.gov/documents/organization/230108.pdf>

<sup>240</sup> Congressional Budget Justification, Appendix 1: Department of State Diplomatic Engagement, Fiscal year 2017, The Secretary of State, accessed May 2, 2017, <https://www.state.gov/documents/organization/252732.pdf>.

## Malaysia Airlines Flight 17 (MH17) Crash Investigation

<b>Actors</b>	<i>Private</i> - Bellingcat, an online investigation hub, the media	<i>Public</i> - Dutch Safety Board (DSB) - Joint Investigation Team (JIT) member states (the Netherlands, Australia, Belgium, Malaysia, and Ukraine) - Public Prosecution Service (Dutch Ministry of Justice)
<b>Actions</b>	- Online intelligence gathering - Publishing of analyses <sup>241</sup>	- Wide spectrum crash investigation <sup>242</sup> and information sharing
<b>Authority</b>	- Reputational	- Dutch Government, JIT member states, UN
<b>Structure</b>	- Independent contributors, <sup>243</sup> ad-hoc, community-driven approach	- Bureaucratic
<b>Norms</b>	- Rules of transparency, verifiability of data	- ICAO standards for evidence collection
<b>Attribution</b>	- Released findings after evidence collection and a review process <sup>244</sup>	- Attribution judgement was released by Public Prosecution Service <sup>245</sup>
<b>Budget and Funding Source(s)</b>	- Total budget unknown - Funded through public pledges, <sup>246</sup> donations, and grants <sup>247</sup>	- 36 million Euro (2014) <sup>248</sup> - Funded by the government of the Netherlands
<b>Best Practices</b>	- <b>Employment of information sharing mechanisms</b> - <b>Engagement of independent international contributors and the pooling of multinational expertise</b> - <b>Adherence to evidence collection methods and standards</b>	- <b>Inter-state collaboration and information exchange</b> - <b>Release of preliminary and final reports</b> - <b>Confidence building measures</b>

<sup>241</sup> "Bellingcat: The home of online investigations," bellingcat.com, accessed May 1, 2017, <https://www.bellingcat.com/?s=MH+17>.

<sup>242</sup> Dutch Safety Board, "Investigation crash MH17, 17 July 2014", accessed May 1, 2017

<https://www.onderzoeksraad.nl/en/onderzoek/2049/investigation-crash-mh17-17-july-2014>.

<sup>243</sup> Cameron Colquhoun, "A Brief History of Open Source Intelligence," bellingcat.com, July 14, 2016, accessed May 2, 2017, <https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/>.

<sup>244</sup> Ben Sullivan, "Bellingcat Wants Your Help to Debunk Fake News," *Vice Motherboard*, March 7, 2017, accessed May 2, 2017, [https://motherboard.vice.com/en\\_us/article/bellingcat-wants-your-help-to-debunk-fake-news](https://motherboard.vice.com/en_us/article/bellingcat-wants-your-help-to-debunk-fake-news).

<sup>245</sup> Lizzie Dearden, "MH17 report: 298 victims remembered as Dutch Safety Board report reveals cause," *The Independent*, October 13, 2015, accessed May 2, 2017, <http://www.independent.co.uk/news/world/europe/mh17-report-names-of-the-298-victims-as-dutch-safety-board-reveals-cause-of-crash-a6691941.html>.

<sup>246</sup> "So how is Bellingcat funded?," *whathappenedtoflightmh17.com*, March 25, 2016, <http://www.whathappenedtoflightmh17.com/so-how-is-bellingcat-funded/>.

<sup>247</sup> *Ibid.*, 111

<sup>248</sup> Igrindstad, "OVER €36M SPENT ON MH17 INVESTIGATION SO FAR," *NL Times*, November 21, 2014, accessed May 2, 2017, <http://nltimes.nl/2014/11/21/eu36m-spent-mh17-investigation-far>.

Actors	<i>Private</i> - Mandiant, private security firms, the media, academia <sup>249</sup>	<i>Public</i>
Actions	- Investigate global attacks, attribute to specific individuals, share actionable information to prevent future attacks <sup>250</sup>	
Authority	- One of the 'Top Four' cybersecurity firms, composed of elite staff <sup>251</sup>	
Structure	- Centralized investigation, peer-review from other security firms and the media	
Norms	- Full-disclosure, technical forensic norms, Information sharing, XML Schema <sup>252</sup>	
Attribution	- Final attribution made in a report, details evidence collection and analysis <sup>253</sup>	
Budget and Funding Source(s)	- Funded by private, for-profit firm	
Best Practices	<ul style="list-style-type: none"> <li>- <b>Public disclosure</b><sup>254</sup></li> <li>- <b>Published analysis of evidence</b></li> <li>- <b>Provided indicators:</b> <ul style="list-style-type: none"> <li>- <b>Domains used by the attacking infrastructure, SSL certs, MDS hashes of APT1 malware, open source 'indicators of compromise'</b><sup>255</sup></li> </ul> </li> </ul>	

<sup>249</sup> Benjamin Wittes, "Mandiant Report on 'APT 1'," *Lawfare.org*, February 20, 2013, accessed April 29, 2017, <https://lawfareblog.com/mandiant-report-apt1>.

<sup>250</sup> William Wan and Ellen Nakashima, "Report ties cyberattacks on U.S. computers to Chinese military," *Washington Post*, January 19, 2013, accessed April 29, 2017, [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](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).

<sup>251</sup> Pia Rivera, "Top Cybersecurity Companies," *INVESTING NEWS*, March 28, 2017, accessed April 29, 2017, <http://investingnews.com/daily/tech-investing/cybersecurity-investing/top-cyber-security-companies/>; Brad Stone and Michael Riley, "Mandiant, the Go-To Security Firm for Cyber-Espionage Attacks," *Bloomberg*, February 8, 2013, accessed April 28, 2017, <https://www.bloomberg.com/news/articles/2013-02-07/mandiant-the-go-to-security-firm-for-cyber-espionage-attacks>.

<sup>252</sup> Wade Williamson, "Lessons from Mandiant's APT1 Report," *SECURITY WEEK*, February 29, 2013, accessed April 29, 2017, <http://www.securityweek.com/lessons-mandiant%E2%80%99s-apt1-report>.

<sup>253</sup> Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," accessed April 29, 2017, <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>; David E. Sanger, David Barboza and Nicole Perloth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *New York Times*, February 29, 2013, accessed April 29, 2017, <https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>.

<sup>254</sup> "APT1: Exposing One of China's Cyber Espionage Units" on YouTube, accessed April 29, 2017, <https://www.youtube.com/watch?v=6p7FqSav6Ho>.

<sup>255</sup> Wade Williamson (2017) at 46.

## Mumbai Terrorist Attack Investigation

<b>Actors</b>	<i>Private</i>	<i>Public</i> - Intelligence agencies of US, United Kingdom, Australia, and Pakistan
<b>Actions</b>		- Conducted a criminal investigation, established cross-border intelligence sharing, and pressured Pakistan to become involved in the investigation <sup>256</sup>
<b>Authority</b>		- Ad-hoc and subjected to the legal authority of countries involved
<b>Structure</b>		- State integrated, non-bureaucratic
<b>Norms</b>		- Not peer-reviewed, but followed standard analysis of forensic evidence, low-degree of transparency, <sup>257</sup> geographic representation
<b>Attribution</b>		- Released findings and specifically attributed attack to a terrorist group, and named individuals behind the planning <sup>258</sup>
<b>Budget and Funding Source(s)</b>		- Unknown
<b>Best Practices</b>		- <b>Information and evidence sharing between multiple nations</b> - <b>Transnational data collection</b>

<sup>256</sup> Sebastian Rotella, James Glanz and David E. Sanger, "In 2008 Mumbai Attacks, Piles of Spy Data, but an Uncompleted Puzzle," *Pro Publica*, December 21, 2014, accessed April 29, 2017, <https://www.propublica.org/article/mumbai-attack-data-an-uncompleted-puzzle>.

<sup>257</sup> Sebastian Rotella, "Four Disturbing Questions About the Mumbai Terror" *FRONTLINE PBS*, February 22, 2013, accessed April 28, 2017, <http://www.pbs.org/wgbh/frontline/article/four-disturbing-questions-about-the-mumbai-terror-attack/>.

<sup>258</sup> *Ibid.*, 115

## Sony Pictures Hack Investigation

<b>Actors</b>	<i>Private</i> - FireEye and Mandiant	<i>Public</i> - FBI
<b>Actions</b>	- Investigated source of attack	- Investigated source of attack
<b>Authority</b>	- Reputational – rose to prominence after implicating Chinese cyberespionage in 2013	- US government
<b>Structure</b>	- Five consulting offerings, “incident response and preparedness lifecycle” <sup>259</sup>	- Cyber division, 56 field offices with cyber teams 93 computer crimes task forces - Partnerships with Department of Defense, Homeland Security) <sup>260</sup>
<b>Norms</b>		- Policies set out by FBI - US law
<b>Attribution</b>	- No direct attribution	- FBI concluded that North Korea is responsible for the attack <sup>261</sup>
<b>Budget and Funding Source(s)</b>	- \$8.6 million (2016) <sup>262</sup> - Funds raised primarily from venture investor	- Budget for this investigation unknown - Funded by Department of Justice <sup>263</sup>
<b>Best Practices</b>	- <b>Called on for most major cybersecurity attacks</b>	- <b>Exemplifies collaboration and cooperation across departments</b>

<sup>259</sup> “Services,” *FireEye*, accessed May 1, 2017, <https://www.fireeye.com/services.html>.

<sup>260</sup> “Cyber Crime,” *Federal Bureau of Investigation*, accessed May 1, 2017, <https://www.fbi.gov/investigate/cyber>.

<sup>261</sup> “FBI Concludes North Korea Responsible for Sony Hack,” *MSNBC*, December 19, 2014, accessed April 29, 2017, <http://www.msnbc.com/msnbc/fbi-concludes-north-korea-responsible-sony-hack>.

<sup>262</sup> “FireEye Reports Fourth Quarter and Fiscal Year 2016 Financial Results (None:FEYE),” *investors.com*, accessed May 1, 2017, <http://investors.fireeye.com/releasedetail.cfm?ReleaseID=1010252>.

<sup>263</sup> “Federal Bureau of Investigation FY 2017 Budget Request at a Glance,” *justice.gov*, accessed April 29, 2017, <https://www.justice.gov/jmd/file/822286/download>.

## Stuxnet Investigation

<b>Actors</b>	<i>Private</i> - Symantec, VirusBlockAda, Kaspersky Labs, McAfee, other security firms, industry and geopolitical experts, the media	<i>Public</i> - NSA, DHS, IAEA
<b>Actions</b>	- Worked on discovery, <sup>264</sup> information sharing, <sup>265</sup> technical analyses, <sup>266</sup> and geopolitical analyses <sup>267</sup>	- NSA employees leaked classified information - IAEA Verified Iran's compliance with the non-proliferation treaty - Provided context to Stuxnet attribution judgements
<b>Authority</b>	- Reputational	- US government, IAEA
<b>Structure</b>	- Ad-hoc <sup>268</sup> with Symantec <sup>269</sup> and Kaspersky Labs <sup>270</sup> taking leadership roles	- Nation-state support was not active or structured in the investigation - All parties were only direct or indirect information providers
<b>Norms</b>	- Information technology community best practices, transparency	- The Statute of IAEA, information confidentiality practices and non-disclosure laws <sup>271</sup>
<b>Attribution</b>	- Final attributional judgements were drawn by media <sup>272</sup> while the firms collected evidence, completed analyses	- Confirmed already established attribution judgments <sup>273</sup>
<b>Budget and Funding Source(s)</b>	- Budget unknown - Each party funded independently	- Total amount is unknown - Not clear whether NSA/DHS employees were compensated
<b>Best Practices</b>	- <b>Information sharing mechanisms</b> - <b>Confidence building</b> - <b>Pooling of multinational expertise</b> - <b>Evidence collection methods</b>	- <b>Information retrieval methods from state entities</b>

<sup>264</sup> VirusBlokAda, "Modules of current malware were first time detected by 'VirusBlokAda' company specialists on the 17th of June 2010...", accessed May 1, 2017, <http://anti-virus.by/en/tempo.shtml>.

<sup>265</sup> Brian Krebs, "Experts Warn of New Windows Shortcut Flaw," *Krebs On Security*, July 10, 2010, accessed May 1, 2017, <http://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/>.

<sup>266</sup> Nicolas Falliere, Liam O Murchu and Eric Chien, "W32. Stuxnet Dossier, version 1.4," *Symantec Security Response* (February, 2011), accessed May 1, 2017, <https://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices>.

<sup>267</sup> Stratfor, "The U.S.-Israeli Stuxnet Alliance," *Stratfor.com*, January 17, 2011, accessed May 1, 2017, <https://www.stratfor.com/analysis/us-israeli-stuxnet-alliance>.

<sup>268</sup> Kim Zetter, "How digital detectives deciphered Stuxnet, the most menacing malware in history," *WIRED*, July 11, 2011, accessed May 1, 2017, <https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/>.

<sup>269</sup> *Ibid.*, 126

<sup>270</sup> David Kushner, "The Real Story of Stuxnet: How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program," *IEEE Spectrum*, February 26, 2013, accessed May 1, 2017, <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

<sup>271</sup> National Security Agency, "NSA/CSS Policy Manual 1-52," May, 23 2014, accessed May 1, 2017, [https://www.nsa.gov/news-features/decclassified-documents/nsa-css-policies/assets/files/Policy\\_Manual\\_1-52.pdf](https://www.nsa.gov/news-features/decclassified-documents/nsa-css-policies/assets/files/Policy_Manual_1-52.pdf).

<sup>272</sup> William J. Broad, John Markoff and David E. Sager, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, accessed May 1, 2017, <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>.

<sup>273</sup> Jason Koebler, "NSA Built Stuxnet, but Real Trick Is Building Crew of Hackers," *U.S. News*, June 8, 2012, accessed May 1, 2017, <https://www.usnews.com/news/articles/2012/06/08/nsa-built-stuxnet-but-real-trick-is-building-crew-of-hackers>.

## 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

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

# Bibliography

- “10 Top Cybersecurity Companies.” *Investing News Network*, March 28, 2017. <http://investingnews.com/daily/tech-investing/cybersecurity-investing/top-cyber-security-companies/>.
- “2016 Global Financial Report.” Accessed April 29, 2017. <https://www.amnesty.org/en/2016-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 13, 2017. <http://www.state.gov/t/avc/rls/rpt/2016/255651.htm>.
- “A Breakdown and Analysis of the December 2014 Sony Hack.” Accessed April 30, 2017. <https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/>.
- “A Day in the Life of a Safeguards Inspector | IAEA.” Accessed May 4, 2017. <https://www.iaea.org/newscenter/news/a-day-in-the-life-of-a-safeguards-inspector>.
- “A New Approach to China.” *Official Google Blog*, May 2, 2017. <https://googleblog.blogspot.com/2010/01/new-approach-to-china.html>.
- “About.” *Join Our Project-Based Initiatives*. Accessed May 2, 2017. <http://www.icao.int/about-icao/partnerships/Pages/default.aspx>.
- “About.” Accessed May 2, 2017. <http://www.icao.int/about-icao/partnerships/Pages/default.aspx>.
- “About Cyber Defence Centre | CCDCOE.” *NATO Cooperative Cyber Defence Centre of Excellence*. Accessed April 30, 2017. <https://ccdcoe.org/about-us.html>.
- “About FINRA | FINRA.org.” Accessed May 2, 2017. <https://www.finra.org/about>.
- “About ICAO.” Accessed May 2, 2017. <http://www.icao.int/about-icao/Pages/default.aspx>.
- “About Our Research.” *Human Rights Watch*, April 21, 2015. <https://www.hrw.org/about-our-research>.
- “About the Citizen Lab,” accessed June 5, 2017, <https://citizenlab.org/about/>
- “Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments.” U.S. Department of State, July 2014. <https://www.state.gov/documents/organization/230108.pdf>.
- 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/](https://fas.org/blogs/secrecy/2008/03/commercial_satellites_as_natio/).
- Ahmed, Azam, “Amid Insider Trading Inquiry, Tiger Asia Calls It Quits,” *New York Times*, August 14, 2012, accessed May 1, 2017, [https://dealbook.nytimes.com/2012/08/14/amid-insider-trading-inquiry-tiger-asia-calls-it-quits/?\\_r=0](https://dealbook.nytimes.com/2012/08/14/amid-insider-trading-inquiry-tiger-asia-calls-it-quits/?_r=0).
- “Air Navigation Commission.” Accessed May 2, 2017. <http://www.icao.int/about-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/>.

- “Amid Insider Trading Inquiry, Tiger Asia Calls It Quits - The New York Times,” May 2, 2017. [https://dealbook.nytimes.com/2012/08/14/amid-insider-trading-inquiry-tiger-asia-calls-it-quits/?\\_r=1](https://dealbook.nytimes.com/2012/08/14/amid-insider-trading-inquiry-tiger-asia-calls-it-quits/?_r=1).
- “An Outline of the FINRA Arbitration Process For Customer-Broker Disputes.” *Smiley Bishop & Porter LLP*, April 20, 2011. <http://www.sbpllp.com/an-outline-of-the-finra-arbitration-process-for-customer-broker-disputes/>.
- “Anti-Money Laundering.” *PwC*. Accessed April 30, 2017. <https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/anti-money-laundering.html>.
- “Approach and Standard.” *Office of the Ombudsperson of the Security Council’s 1267 Committee*. <https://www.un.org/sc/suborg/en/ombudsperson/approach-and-standard>.
- “APT1: Exposing One of China’s Cyber Espionage Units.” Accessed April 29, 2017. <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>.
- “APT1: Exposing One of China’s Cyber Espionage Units - YouTube,” May 2, 2017. <https://www.youtube.com/watch?v=6p7FqSav6Ho>.
- “APT 28: A Window Into Russia’s Cyber Espionage Operations?” *FireEye*, October 2014.
- “Asia Times Online: Korea News and Korean Business and Economy, Pyongyang News,” May 2, 2017. <http://www.atimes.com/atimes/Korea/LE05Dg01.html>.
- “‘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 | Technology | The Guardian.” *The Guardian*, June 5, 2014. <https://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents>.
- Barrett, Devlin. “FBI Says North Korea Behind Sony Hack.” *Wall Street Journal*, December 19, 2014, sec. US. <http://www.wsj.com/articles/fbi-says-north-korea-behind-sony-hack-1419008924>.
- Baruah, Amit. “Pakistan ‘Shared Mumbai Attacks Research with India’ - BBC News,” December 4, 2010. <http://www.bbc.com/news/world-south-asia-11917514>.
- BPR Administration, “BPR Interview: Citizens Lab Director Ronald Deibert,” *Brown Political Review*, October 21, 2012, accessed June 5, 2017, <http://www.brownpoliticalreview.org/2012/10/interview-citizens-lab-director-ronald-deibert/>.
- Bright, Arthur. “Estonia Accuses Russia of ‘Cyberattack.’” *Christian Science Monitor*, May 17, 2007. Accessed May 17, 2017. <https://www.csmonitor.com/2007/0517/p99s01-duts.html>.
- Broad, William J., and John Markoff, and David E. Sanger. “Israel Tests on Worm Called Crucial in Iran Nuclear Delay,” *New York Times*, January 15, 2011. Accessed May 23, 2017, [https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?\\_r=1&ref=general&src=me&pagewanted=all](https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&ref=general&src=me&pagewanted=all).

- Broggi, Jeremy. "Building on Executive Order 13,636 To Encourage Information Sharing for Cybersecurity Purposes." Accessed May 24, 2017. [http://www.harvard-ilpp.com/wp-content/uploads/2014/05/37\\_2\\_653\\_Broggi.pdf](http://www.harvard-ilpp.com/wp-content/uploads/2014/05/37_2_653_Broggi.pdf).
- "Budget of the Organization 2017-2018-2019." Montreal: ICAO, October 2016. [http://www.icao.int/publications/Documents/10074\\_en.pdf](http://www.icao.int/publications/Documents/10074_en.pdf).
- "Building Public Trust in Nuclear Power." International Atomic Energy Agency, March 2013. <https://www.iaea.org/sites/default/files/publications/magazines/bulletin/bull54-1/54104711212.pdf>
- Carr, Jeffrey. "Responsible Attribution: A Prerequisite for Accountability." *NATO CCD COE, The Tallinn Papers*, no. No.6 (2014): 1–8. <https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%206%20Carr.pdf>.
- Carlin, John P., "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats." Accessed May 17, 2017. *Harvard National Security Journal/Vol. 7*. <https://docs.google.com/viewer?docex=1&url=https://lawfare.s3-us-west-2.amazonaws.com/staging/2016/Carlin%20FINAL.pdf>.
- "CETS 005 - Convention for the Protection of Human Rights and Fundamental Freedoms - 1680063765." Accessed May 17, 2017. <https://rm.coe.int/1680063765>.
- "CFT Cases - The Egmont Group." Accessed April 3, 2017. <https://egmontgroup.org/en/document-library/12>.
- "Chapter I | United Nations." Accessed May 4, 2017. <http://www.un.org/en/sections/un-charter/chapter-i/index.html>.
- Charney, Scott, Erin English, Aaron Kleiner, Nemanja Malisevic, Angela McKay, Jan Neutze, and Paul Nicholas. "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms," June 2016. [https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms\\_vFinal.pdf](https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf).
- Chayes, Abram, and Antonia Handler Chayes. *The New Sovereignty: Compliance with International Regulatory Agreements*. Harvard University Press, 1998. <https://www.amazon.com/New-Sovereignty-Compliance-International-Regulatory/dp/0674617835>.
- "China's Internet: The Great Firewall." *The Economist*, April 6, 2013. <http://www.economist.com/news/special-report/21574631-chinese-screening-online-material-abroad-becoming-ever-more-sophisticated>.
- "Citizen Lab | Github," accessed June 7, 2017, <https://github.com/citizenlab>.
- Clark, David, and Susan Landau. "Untangling Attribution." Massachusetts Institute of Technology, 2011. <http://static.cs.brown.edu/courses/csci1950-p/sources/lec12/ClarkandLandau.pdf>.
- "Clinton's Speech on Internet Freedom, January 2010." *Council on Foreign Relations*, May 2, 2017. <http://www.cfr.org/internet-policy/clintons-speech-internet-freedom-january-2010/p21253>.
- "Create a Strategic Outreach Campaign to Add Value to Your Organization." *Prowl*, May 23, 2011. <http://prowlpublicrelations.blogspot.com/2011/06/create-strategic-outreach-campaign-to.html?m=0>.

- Colquhoun, Cameron. "A Brief History of Open Source Intelligence." *Bellingcat*, July 14, 2016. <https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/>.
- "Commercial Child Pornography: A Brief Snapshot of the Financial Coalition Against Child Pornography." National Center for Missing and Exploited Children, 2016. [http://www.missingkids.com/en\\_US/documents/Commercial\\_child\\_pornography\\_-\\_A\\_brief\\_snapshot\\_of\\_the\\_FCACP\\_2016.pdf](http://www.missingkids.com/en_US/documents/Commercial_child_pornography_-_A_brief_snapshot_of_the_FCACP_2016.pdf).
- "Congressional Budget Justification, Appendix 1: Department of State Diplomatic Engagement, Fiscal Year 2017." The Secretary of State. Accessed May 2, 2017. <https://www.state.gov/documents/organization/252732.pdf>.
- "Crash MH17." *Politie (Police)*. Accessed May 1, 2017. <https://www.politie.nl/themas/flight-mh17-2.html>.
- "Crash of Malaysia Airlines Flight MH17." Dutch Safety Board, October 22, 2015. <https://onderzoeksraad.nl/uploads/phase-docs/1006/debcd724fe7breport-mh17-crash.pdf>.
- "Crash of Malaysia Airlines Flight MH17, Final Report." Dutch Safety Board, October 22, 2015. <https://www.onderzoeksraad.nl/uploads/phase-docs/1006/debcd724fe7breport-mh17-crash.pdf>.
- "Cross-Border Implications of The SEC Whistleblower Report." *Law360*, May 2, 2017. <https://www.law360.com/articles/395744/cross-border-implications-of-the-sec-whistleblower-report>.
- "Cyber Crime." *Federal Bureau of Investigation*. Accessed May 1, 2017. <https://www.fbi.gov/investigate/cyber>.
- "Cyber Crime — FBI." Accessed April 13, 2017. <https://www.fbi.gov/investigate/cyber>.
- Cyberattack on Google Said to Hit Password System - The New York Times," May 2, 2017. <http://www.nytimes.com/2010/04/20/technology/20google.html>.
- "Cybersecurity | Homeland Security." Accessed April 13, 2017. <https://www.dhs.gov/topic/cybersecurity>.
- "Cyber-Security Task Force: Public-Private Information Sharing," Bipartisan Policy Review, July 2012. Accessed May 17, 2017. [http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/PublicPrivate Information Sharing.pdf](http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/PublicPrivate%20Information%20Sharing.pdf)
- "Cyber Stewards," accessed June 7, 2017, <https://cyberstewards.org/>
- Cyranoski, David. "Controversy over South Korea's sunken ship," *Nature Journal*, July 14, 2010. Accessed May 22, 2017. <http://www.nature.com/news/2010/100708/full/news.2010.343.html>.
- "Data Privacy Laws Around the World," *Baker McKenzie* (2016). Accessed May 23, 2017, <https://globalcompliancenews.com/data-privacy/data-privacy-laws-around-the-world/>.
- Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *WIRED*. Accessed May 17, 2017. <https://www.wired.com/2007/08/ff-estonia/>.
- Dearden, Lizzie. "MH17 Report: 298 Victims Remembered as Dutch Safety Board Report Reveals Cause." *INDEPENDENT*, October 13, 2015. <http://www.independent.co.uk/news/world/europe/mh17-report-names-of-the-298-victims-as-dutch-safety-board-reveals-cause-of-crash-a6691941.html>.

Demick, Barbara, and John M. Glionna, "Doubts Surface on North Korea's Role in Ship Sinking." *Los Angeles Times*, July 23, 2010. <http://articles.latimes.com/2010/jul/23/world/la-fg-korea-torpedo-20100724>.

"Department of Safeguards." Text, July 26, 2016. <https://www.iaea.org/about/organizational-structure/department-of-safeguards>.

"Department of Technical Cooperation." Text, August 17, 2016. <https://www.iaea.org/about/organizational-structure/department-of-technical-cooperation>.

"Did an American Mine Sink South Korean Ship? - New America Media," May 2, 2017. <http://newamericamedia.org/2010/05/did-an-american-mine-sink-the-south-korean-ship.php>.

"EFC Members." *European Financial Coalition against Commercial Sexual Exploitation of Children Online*, n.d. [http://www.europeanfinancialcoalition.eu/efc\\_members.php](http://www.europeanfinancialcoalition.eu/efc_members.php).

"Egmont Group Communication Strategy." Egmont Group of Financial Intelligence Units, July 2015. <https://egmontgroup.org/en/document-library/8>

Elash, Anita, "How The Citizen Lab polices the world's digital spies," *CS Monitor*, December 22, 2016, accessed June 7, 2017, <http://www.csmonitor.com/World/Passcode/2016/1222/How-The-Citizen-Lab-polices-the-world-s-digital-spies>.

"Enter the Cyber-Dragon | Vanity Fair," May 2, 2017. <http://www.vanityfair.com/news/2011/09/chinese-hacking-201109>.

"Estonia Fines Man for 'Cyber War.'" *BBC News*, January 25, 2008. <http://news.bbc.co.uk/2/hi/technology/7208511.stm>.

"Ex-Pres. Secretary Sued for Spreading Cheonan Rumors," *The Dong-A Ilbo (English Edition)*, May 8, 2010. Accessed May 22, 2017, <http://english.donga.com/List/3/all/26/264989/1>

Falliere, Nicolas. "Stuxnet Introduces the First Known Rootkit for Industrial Control Systems." *Symantec Blog*, August 6, 2010. <https://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices>.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. Stuxnet Dossier, Version 1.4." Symantec Security Response, February 2011. <https://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices>.

"FATF-GAFI.ORG - Financial Action Task Force (FATF)." Accessed April 3, 2017. <http://www.fatf-gafi.org/>.

"FBI Concludes North Korea Responsible for Sony Hack." *MSNBC*, December 19, 2014. <http://www.msnbc.com/msnbc/fbi-concludes-north-korea-responsible-sony-hack>.

"FBI Offers New Evidence Connecting North Korea To Sony Hack." *NPR.org*. Accessed April 30, 2017. <http://www.npr.org/2015/01/07/375671935/fbi-offers-new-evidence-connecting-north-korea-to-sony-hack>.

"Federal Bureau of Investigation - Facts & Figures." Accessed April 30, 2017. [https://www2.fbi.gov/facts\\_and\\_figures/accountability\\_compliance.htm](https://www2.fbi.gov/facts_and_figures/accountability_compliance.htm).

"Federal Bureau of Investigation FY 2017 Budget Request at a Glance," n.d. <https://www.justice.gov/jmd/file/822286/download>.

Federal Bureau of Investigation, and U.S. Department of Homeland Security. "GRIZZLY STEPPE-Russian Malicious Cyber Activity." Joint Analysis U.S. Government Report, December 29, 2016.

"Financial Intelligence Units: An Overview," International Monetary Fund, and World Bank. 2004. <https://www.imf.org/external/pubs/ft/FIU/fiu.pdf>.

"Financial Intelligence Units (FIUs) - The Egmont Group." Accessed April 3, 2017. <https://www.egmontgroup.org/en/content/financial-intelligence-units-fius>.

"FINRA 2015 Exams: Variable Annuities." Regulatory Brief: A Publication of PwC's Financial Services Regulatory Practice, January 2015. <http://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/finra-exams-variable-annuities.pdf>.

"FINRA Board of Governors | FINRA.org." Accessed May 2, 2017. <https://www.finra.org/about/finra-board-governors>.

"FireEye | Crunchbase." Accessed April 30, 2017. <https://www.crunchbase.com/organization/fireeye>.

"FireEye Reports Fourth Quarter and Fiscal Year 2016 Financial Results (None:FEYE)." Accessed May 1, 2017. <http://investors.fireeye.com/releasedetail.cfm?ReleaseID=1010252>.

Flintoff, Corey. "Kaspersky Lab: Based in Russia, Doing Cybersecurity in the West." *NPR*, August 10, 2015. <http://www.npr.org/sections/alltechconsidered/2015/08/10/431247980/kaspersky-lab-a-cybersecurity-leader-with-ties-to-russian-govt>.

"FOIA.gov - Freedom of Information Act: Where to Make a FOIA Request." Accessed April 17, 2017. <https://www.foia.gov/report-makerequest.html>.

"Functions and Powers of the United Nations Security Council." Accessed May 3, 2017. <http://www.un.org/en/sc/about/functions.shtml>.

"FY 2017 President's Budget." Financial Crimes Enforcement Network (FinCEN, February 9, 2016. <https://www.treasury.gov/about/budget-performance/CJ17/14.%20FinCEN%20FY%202017%20CJ.PDF>.

Gagnon, Gary. "Why Businesses Should Share Intelligence About Cyber Attacks." *Harvard Business Review*, June 13, 2013. <https://hbr.org/2013/06/why-businesses-should-share-intelligence-abo>.

Galperin, Eva, Marquis-Borire, Morgan, and Scott-Railton, John, "Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns," Citizen Lab-EEF, December 23, 2013, accessed June 7, 2017, <https://www.eff.org/document/quantum-surveillance-familiar-actors-and-possible-false-flags-syrian-malware-campaigns>.

"General Assembly, on Fifth Committee's Recommendation, Adopts Raft of Texts on 2014-2015 Biennium Budget Appropriations, Common System, Peacekeeping." *United Nations*, <https://www.un.org/press/en/2014/ga11608.doc.htm>.

Gierow, Hauke Johannes. "Cyber Security in China: Internet Security, Protectionism and Competitiveness. New Challenges to Western Businesses." MERICS, April 22, 2015. Accessed May 17, 2017. [http://www.merics.org/fileadmin/templates/download/china-monitor/150407\\_MERICS\\_China\\_Monitor\\_twenty-two\\_en.pdf](http://www.merics.org/fileadmin/templates/download/china-monitor/150407_MERICS_China_Monitor_twenty-two_en.pdf).

Gladstone, Rick, and David E. Sanger. "New Sanctions on North Korea Over Nuclear Test." *The New York Times*, March 7, 2013.

- <http://www.nytimes.com/2013/03/08/world/asia/north-korea-warns-of-pre-emptive-nuclear-attack.html>.
- Glazer, Emily, and Christina Rexrode. "Wells Fargo Fined for Anti-Money- Laundering 'Failures.'" *Wall Street Journal*, December 18, 2014, sec. Markets.  
<http://www.wsj.com/articles/wells-fargo-fined-for-anti-money-laundering-failures-1418913816>.
- Goldsmith, Jack. "Toward Greater Transparency of National Security Legal Work," (May 2015).  
<http://jackgoldsmith.org/toward-greater-transparency-of-national-security-legal-work/>.
- Goodin, Dan. "Kaspersky Lab's Top Investigator Reportedly Arrested in Treason Probe." *ArsTechnica*, January 25, 2017. <https://arstechnica.com/security/2017/01/kaspersky-labs-top-investigator-reportedly-arrested-in-treason-probe/>.
- Goodman, Marc. *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do about It*. First ed. New York: Doubleday, 2015.
- "Google Hackers Had Ability to Alter Source Code | WIRED," May 2, 2017.  
<https://www.wired.com/2010/03/source-code-hacks>.
- "Google's Secret NSA Alliance: The Terrifying Deals between Silicon Valley and the Security State - Salon.com," May 2, 2017.  
[http://www.salon.com/2014/11/16/googles\\_secret\\_nsa\\_alliance\\_the\\_terrifying\\_deals\\_between\\_silicon\\_valley\\_and\\_the\\_security\\_state/](http://www.salon.com/2014/11/16/googles_secret_nsa_alliance_the_terrifying_deals_between_silicon_valley_and_the_security_state/)
- "Government's Recent Labour Interventions Highly Unusual, Experts Say." *CBC News*. Accessed May 3, 2017. <http://www.cbc.ca/news/canada/government-s-recent-labour-interventions-highly-unusual-experts-say-1.977658>.
- "Greenpeace International Annual Report 2015." *Greenpeace International*. Accessed April 27, 2017.  
<http://www.greenpeace.org/international/Global/international/publications/greenpeace/2016/2015-Annual-Report-Web.pdf>.
- "Greenpeace Structure and Organization." *Greenpeace International*. Accessed May 3, 2017.  
<http://www.greenpeace.org/international/en/about/how-is-greenpeace-structured/>.
- "Greenpeace Victories and Successes." Accessed May 4, 2017.  
<http://www.greenpeace.org/international/Global/international/code/2016/victory-timeline/index.html>.
- "Guidelines of the Committee for the Conduct of Its World." United Nations Security Council, December 23, 2016.  
[https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/guidelines\\_of\\_the\\_committee\\_for\\_the\\_conduct\\_of\\_its\\_work.pdf](https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/guidelines_of_the_committee_for_the_conduct_of_its_work.pdf).
- Gross, Doug. "Google vs. China: Free Speech, Finances or Both? - CNN.com," January 13, 2010.  
<http://www.cnn.com/2010/TECH/01/13/google.china.analysis/index.html>.
- Gross, Michael Joseph. "A Declaration of Cyber-War," *Vanity Fair*, April 2011. Accessed May 23, 2017.  
<https://www.vanityfair.com/news/2011/03/stuxnet-201104>.
- Haggard, Stephan, and Jon R. Lindsay. "North Korea and the Sony Hack: Exporting Instability Through Cyberspace." *AsiaPacific Issues*, no. 117 (May 2015): 1–8.
- Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." *Atlantic Council*, Cyber Statecraft Initiative, 2011.

- [http://www.atlanticcouncil.org/images/files/publication\\_pdfs/403/022212\\_ACUS\\_NatIR\\_responsibilityCyber.PDF](http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatIR_responsibilityCyber.PDF).
- Hesseldahl, Arik. "Sony Pictures Investigates North Korea Link In Hack Attack." *Recode*, November 28, 2014. <https://www.recode.net/2014/11/28/11633356/sony-pictures-investigates-north-korea-link-in-hack-attack>.
- Holgate, Jon Wolfsthal, and Laura S. H. "Cutting Funding to the IAEA Is a Horrible Idea." *Carnegie Endowment for International Peace*. Accessed May 3, 2017. <http://carnegieendowment.org/2017/03/27/cutting-funding-to-iaea-is-horrible-idea-pub-68413>.
- "How Did N.Korea Sink the Cheonan?," May 2, 2017. [http://english.chosun.com/site/data/html\\_dir/2010/05/21/2010052100698.html](http://english.chosun.com/site/data/html_dir/2010/05/21/2010052100698.html).
- Hunker, Jeffrey, Bob Hutchinson, and Jonathan Margulies. "Role and Challenges for Sufficient Cyber-Attack Attribution." *Institute for Information Infrastructure Protection*, January 2008. <http://www.scis.nova.edu/%7Ecannady/ARES/hunker.pdf>.
- "IAEA Budget." Text, June 8, 2016. <https://www.iaea.org/about/overview/budget>.
- "IAEA Safety Standards." Accessed May 2, 2017. <http://www-ns.iaea.org/standards/>.
- Ians. "Kaspersky Lab Joins Interpol-Led Cybercrime Operation across Asian Nations." *The Economic Times*, April 25, 2017. <http://economictimes.indiatimes.com/tech/internet/kaspersky-lab-joins-interpol-led-cybercrime-operation-across-asean-nations/articleshow/58360723.cms>.
- "ICAO: Frequently Asked Questions." Accessed May 2, 2017. <http://www.icao.int/about-icao/FAQ/Pages/icao-frequently-asked-questions-faq-2.aspx>.
- "ICAO's Policies on Charges for Airports and Air Navigation Services." Eighth Edition. Montreal, Quebec, Canada: ICAO, 2009. [http://www.icao.int/publications/Documents/9082\\_8ed\\_en.pdf](http://www.icao.int/publications/Documents/9082_8ed_en.pdf).
- "ICAO's Response to Global Challenges." ICAO. Accessed April 29, 2017. <http://www.icao.int/Newsroom/News%20Doc/copenhaguen-complete134ec9.pdf>.
- "IEWG Plan on a Page." *Egmont Group*, 2016. <https://www.egmontgroup.org/sites/default/files/IEWG%20Plan%20on%20a%20page%2016082016.pdf>.
- Igrindstad. "OVER €36M SPENT ON MH17 INVESTIGATION SO FAR." *NL Times*, November 21, 2014. <http://nltimes.nl/2014/11/21/eu36m-spent-mh17-investigation-far>.
- "ILO Declaration on Fundamental Principles and Rights at Work (DECLARATION)." Accessed May 3, 2017. <http://www.ilo.org/declaration/lang--en/index.htm>.
- "Information Exchange Working Group," n.d. <https://www.egmontgroup.org/sites/default/files/IEWG%20Plan%20on%20a%20page%2016082016.pdf>.
- "Intermediate-Range Nuclear Forces Treaty (INF Treaty)." *U.S. Department of State*. Accessed April 10, 2017. <http://www.state.gov/t/avc/trty/102360.htm>.
- "International Atomic Energy Agency (IAEA) 'Lacks Transparency', Agency's Secrecy | Global Research - Centre for Research on Globalization." Accessed May 3, 2017. <http://www.globalresearch.ca/international-atomic-energy-agency-lacks-transparency-observers-and-researchers-say/5446187>.
- "International Labor Conference," <http://www.ilo.org/>.

- “International Labour Conference.” Accessed May 3, 2017. <http://ilo.org/global/about-the-ilo/how-the-ilo-works/international-labour-conference/lang--en/index.htm>.
- “International Labour Organization.” Accessed May 3, 2017. <http://www.ilo.org/global/lang--en/index.htm>.
- “International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.” The FATF Recommendations. FATF, February 2012. [http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF\\_Recommendations.pdf](http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf).
- “International Union of Pure & Applied Chemistry.” IUPAC | International Union of Pure and Applied Chemistry. Accessed April 28, 2017. <https://iupac.org/who-we-are/>.
- "Inspection and Enforcement by the Regulatory Body." 4.1.3.2. Methods of Inspection. Accessed May 11, 2017. <https://www.iaea.org/ns/tutorials/regcontrol/inspect/insp4133.htm>.
- “Intelligence Community Directive 209-Tearline Production and Dissemination.” Accessed May 25, 2017. <https://fas.org/irp/dni/icd/icd-209.pdf>.
- “Investigation Result on the Sinking of ROKS ‘Cheonan.’” Accessed May 2, 2017. [http://news.bbc.co.uk/nol/shared/bsp/hi/pdfs/20\\_05\\_10jigreport.pdf](http://news.bbc.co.uk/nol/shared/bsp/hi/pdfs/20_05_10jigreport.pdf).
- “Investigation MH17 Crash, July 2014.” Dutch Safety Board. Accessed May 1, 2017. <https://www.onderzoeksraad.nl/en/onderzoek/2049/investigation-crash-mh17-17-july-2014>.
- “IUPAC and the Organisation for the Prohibition of Chemical Weapons Take Partnership to New Level | International Union of Pure and Applied Chemistry.” IUPAC | International Union of Pure and Applied Chemistry, December 1, 2016. <https://iupac.org/iupac-opcw-take-partnership-new-level/>.
- Jakobi, Anja. “Non-State Actors and Global Crime Governance: Explaining the Variance of Public-Private Interaction.” *The British Journal of Politics and International Relations* 18, no. 1 (2016): 72–89.
- Jason Rivera, and Forrest Hare. “The Deployment of Attribution Agnostic Cyberdefense Constructs and Internally Based Cyberthreat Countermeasures.” *CCD COE*, 6th International Conference on Cyber Conflict, 2014, 100–116.
- Johnson, Chris and Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. “Guide to Cyber Threat Information Sharing,” *National Institute of Standards and Technology (NIST)*, April 2016. [http://csrc.nist.gov/publications/drafts/800-150/sp800\\_150\\_second\\_draft.pdf](http://csrc.nist.gov/publications/drafts/800-150/sp800_150_second_draft.pdf).
- Kaytal, Neal. “Community Self Help.” *Georgetown University Law Center Journal of Law, Economics and Policy*, 2005. <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1532&context=facpub>.
- Keizer, Gregg. “Is Stuxnet the ‘Best’ Malware Ever?” *InfoWorld*, September 16, 2010. <http://www.infoworld.com/article/2626009/malware/is-stuxnet-the--best--malware-ever-.html>.
- Kim, Hwang Su, and Mauro Caresta. "What Really Caused the ROKS Cheonan Warship Sinking?" *Advances in Acoustics and Vibration* (2014). Accessed May 22, 2017. <https://www.hindawi.com/journals/aav/2014/514346/>.

- Koebler, Jason. "NSA Built Stuxnet, but Real Trick Is Building Crew of Hackers." *U.S. News*, June 8, 2012. <https://www.usnews.com/news/articles/2012/06/08/nsa-built-stuxnet-but-real-trick-is-building-crew-of-hackers>.
- Koh, Harold Hongju. "Why Do Nations Obey International Law?," Yale Faculty Scholarship Press (1997). Accessed May 23, 2017. [http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2897&context=fss\\_papers](http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2897&context=fss_papers).
- Krebs, Brian. "Experts Warn of New Windows Shortcut Flaw." *Krebs On Security: In-Depth Security News and Investigation*, July 10, 2010. <http://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/>.
- Kurtas, Susan. "Research Guides: UN Documentation: Security Council: Introduction." Research guide. Accessed May 3, 2017. <http://research.un.org/en/docs/sc/introduction>.
- Kushner, David. "The Real Story of Stuxnet: How Kaspersky Lab Tracked down the Malware That Stymied Iran's Nuclear-Fuel Enrichment Program." *EEE Spectrum*, February 26, 2013. Accessed May 17, 2017. <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.
- Landler, Mark. "Diplomatic Storm Brewing Over Korean Peninsula." *The New York Times*, May 19, 2010. <http://www.nytimes.com/2010/05/20/world/asia/20dipl.html>.
- "Latest News and Highlights." Accessed May 2, 2017. <http://www.icao.int/newsroom/Pages/default.aspx>.
- "Lessons from Mandiant's APT1 Report | SecurityWeek.Com." Accessed May 2, 2017. <http://www.securityweek.com/lessons-mandiant%E2%80%99s-apt1-report>.
- "Letter Dated 4 June 2010 from the Permanent Representative of the Republic of Korea to the United Nations Addressed to the President of the Security Council." United Nations Security Council, June 4, 2010. [http://www.un.org/en/sc/repertoire/2010-2011/Part%20I/2010-2011\\_letterKorea.pdf](http://www.un.org/en/sc/repertoire/2010-2011/Part%20I/2010-2011_letterKorea.pdf).
- Lin, Herbert S. "Attribution of Malicious Cyber Incidents: From Soup to Nuts." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, September 2, 2016. <https://papers.ssrn.com/abstract=2835719>.
- Lindsay, Jon R. "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack," *Journal of Cybersecurity* 1 (1): 115, 2015, <http://cybersecurity.oxfordjournals.org/content/1/1/53>
- Lipton, Eric, David E. Sanger, and Scott Shane. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S. - The New York Times." *The New York Times*, December 13, 2016. [https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?\\_r=0](https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0).
- "List of Participating International Organizations and Industry." Accessed May 2, 2017. <http://www.icao.int/Meetings/ICAN2015/Pages/List-of-Participating-Industry-and-International-Organizations.aspx>.
- MacAfee Report, THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE, *Center for Strategic and International Studies*, (July, 2013). <https://docs.google.com/viewer?docex=1&url=http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf>.
- "Making an ICAO Standard." Accessed May 2, 2017. <http://www.icao.int/safety/airnavigation/Pages/standard.aspx#4>.

“Mandiant Report on ‘APT1.’” *Lawfare*, February 20, 2013. <https://lawfareblog.com/mandiant-report-apt1>.

“Mandiant, the Go-To Security Firm for Cyber-Espionage Attacks - Bloomberg,” May 2, 2017. <https://www.bloomberg.com/news/articles/2013-02-07/mandiant-the-go-to-security-firm-for-cyber-espionage-attacks>.

“Membership and Functions.” *Organization for the Prohibition of Chemical Weapons*, <https://www.opcw.org/about-opcw/executive-council/membership-and-functions/>.

“Member States’ Competent Authorities.” Accessed May 3, 2017. <http://www-ns.iaea.org/tech-areas/emergency/member-states-competent-authorities.asp?s=1>.

“Members of the United Nations Security Council.” Accessed May 3, 2017. <http://www.un.org/en/sc/members/>.

“Mission & Priorities.” Folder. *Federal Bureau of Investigation*. Accessed May 1, 2017. <https://www.fbi.gov/about/mission>.

“Mission and Impact of the ILO.” Accessed May 3, 2017. <http://ilo.org/global/about-the-ilo/mission-and-objectives/lang--en/index.htm>.

“Money Laundering and the Financing of Terrorism.” *Egmont Group*, n.d. <https://www.egmontgroup.org/en/content/money-laundering-and-financing-terrorism>.

“Money Laundering and the Financing of Terrorism - The Egmont Group.” Accessed April 30, 2017. <https://egmontgroup.org/en/content/money-laundering-and-financing-terrorism>.

Morris, Harvey. “N Korea Escapes Blame over Ship Sinking.” *Financial Times*, July 9, 2010. <https://www.ft.com/content/4208c344-8b6e-11df-ab4d-00144feab49a>.

“Most S. Koreans Skeptical About Cheonan Findings, Survey Shows.” *The Chosun Ilbo (English Edition)*, September 8, 2010. Accessed May 17, 2017. [http://english.chosun.com/site/data/html\\_dir/2010/09/08/20100908000979.html](http://english.chosun.com/site/data/html_dir/2010/09/08/20100908000979.html).

Nakashima, Ellen. “Stuxnet was work of U.S. and Israeli experts, officials say,” *The Washington Post*, June 2, 2012. Accessed May 23, 2017. [https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U\\_story.html](https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html).

“News | FinCEN.gov.” Accessed April 30, 2017. <https://www.fincen.gov/news-room/news>.

“News from the EFC: The Past, The Present, The Future.” Accessed April 28, 2017. <http://us11.campaign-archive1.com/?u=a39d608c8102dd5c712efbc48&id=d1ce5b24df>.

Nikitin, Mary Beth, Mark E. Manyin, Emma Chanlett-Avery, and Dick K. Nanto. “North Korea’s Second Nuclear Test: Implications of U.N. Security Council Resolution 1874.” Congressional Research Service, April 15, 2010. <https://fas.org/sgp/crs/nuke/R40684.pdf>.

“North Korea Threatens ‘All-out War’ over Warship Sinking Report - Telegraph,” May 2, 2017. <http://www.telegraph.co.uk/news/worldnews/asia/northkorea/7745370/North-Korea-threatens-all-out-war-over-warship-sinking-report.html>.

Oatley, Thomas H. *Debates in International Political Economy*. Boston: Longman, 2012.

“Observers and International Partners - The Egmont Group.” Accessed April 3, 2017. <https://egmontgroup.org/en/document-library/13>.

Office of the Director of National Intelligence. “Background to ‘Assessing Russian Activities and Intentions in Recent US Elections’: The Analytic Process and Cyber Incident Attribution.” U.S. Government. National Intelligence Council, January 6, 2017.

- “OHCHR | International Covenant on Civil and Political Rights.” 1966. Accessed May 18, 2017. <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>.
- “One or More Unknown Traders in the Securities of Fortress Investment Group, LLC (Release No. LR-23760; Feb. 28, 2017).” Accessed May 2, 2017. <https://www.sec.gov/litigation/complaints/2017/comp23760.pdf>.
- “OPCW Calendar of Events.” *Organization for the Prohibition of Chemical Weapons*. <https://www.opcw.org/events-calendar/>.
- “OPCW.” OPCW. Accessed April 13, 2017. <https://opcw.unmissions.org/>.
- “OPCW Mission Statement.” *Organization for the Prohibition of Chemical Weapons*, n.d. <https://www.opcw.org/about-opcw/mission/>.
- “OPCW Press Release on Allegations of Chemical Weapons Use in Southern Idli, Syria.” *Organization for the Prohibition of Chemical Weapons*, April 4, 2017.
- “Open Net Initiative,” accessed June 7, 2017, <https://opennet.net/>.
- “Organization for the Prohibition of Chemical Weapons.” *NIT: Building a Safer World*, April 28, 2017. <http://www.nti.org/learn/treaties-and-regimes/organization-for-the-prohibition-of-chemical-weapons/>.
- “Our Code of Ethics & Business Conduct: Living Our Vision & Values.” Wells Fargo. Accessed April 30, 2017. <https://www08.wellsfargomedia.com/assets/pdf/about/corporate/code-of-ethics.pdf>.
- “Our Core Values | Greenpeace International.” Accessed May 4, 2017. <http://www.greenpeace.org/international/en/about/our-core-values/>.
- “Our Ships | Greenpeace International.” Accessed May 4, 2017. <http://www.greenpeace.org/international/en/about/ships/>.
- Patel, Neil. “Why a Transparent Culture Is Good for Business.” *Fast Company*, October 9, 2014. <https://www.fastcompany.com/3036794/why-a-transparent-culture-is-good-for-business>.
- Parket, Landelrijk. “JIT: Flight MH17 Was Shot down by a BUK Missile from a Farmland near Pervomaiskyi.” *Openbaar Ministerie*, September 28, 2016. <https://www.om.nl/onderwerpen/mh17-crash/@96068/jit-flight-mh17-shot/>.
- Parket, Landelrijk. “Joint Investigation Team’s Reaction to OVV Report.” *Openbaar Ministerie*, October 13, 2015. <https://www.om.nl/onderwerpen/mh17-crash/@91208/joint-investigation-0/>.
- “Procedure.” *Office of the Ombudsperson of the Security Council’s 1267 Committee*, n.d. <https://www.un.org/sc/suborg/en/ombudsperson/procedure>.
- “Programme and Budget.” Accessed May 3, 2017. <http://embargo.ilo.org/global/about-the-ilo/how-the-ilo-works/programme-and-budget/lang--en/index.htm>.
- “Proposing a Self-Help Privilege for Victims of Cyber Attacks,” May 2, 2017. [https://www.researchgate.net/publication/298414555\\_Proposing\\_a\\_Self-Help\\_Privilege\\_for\\_Victims\\_of\\_Cyber\\_Attacks](https://www.researchgate.net/publication/298414555_Proposing_a_Self-Help_Privilege_for_Victims_of_Cyber_Attacks).
- “Protecting and Defending against Cyberthreats in Uncertain Times | USA 2017 | RSA Conference.” Accessed May 23, 2017. <http://www.rsaconference.com/events/us17/agenda/sessions/7577-keynote-speaker-brad-smith-president-and-chief>.

- “Public Statements and Communiques - The Egmont Group.” Accessed April 3, 2017.  
<https://www.egmontgroup.org/en/document-library/9>.
- “Q&A about SecureDrop on The Washington Post.” *Washington Post*, June 5, 2014.  
<https://www.washingtonpost.com/pr/wp/2014/06/05/qa-about-securedrop-on-the-washington-post/>.
- “Report Ties Cyberattacks on U.S. Computers to Chinese Military - The Washington Post,” May 2, 2017. [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](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).
- “Reports | United Nations Security Council Subsidiary Organs.” Accessed May 24, 2017.  
[https://www.un.org/sc/suborg/en/sanctions/1718/panel\\_experts/reports](https://www.un.org/sc/suborg/en/sanctions/1718/panel_experts/reports).
- Resolution 1718 (2006), S/RES/1718 (2006) § (2006).  
<https://www.globalpolicy.org/images/pdfs/1014reso1718.pdf>.
- “Resolution 2253 (2015).” United Nations Security Council, December 17, 2015.  
[http://www.un.org/en/ga/search/view\\_doc.asp?symbol=S/RES/2253\(2015\)](http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2253(2015)).
- “Results Confirm North Korea Sank Cheonan- Daily NK,” May 2, 2017.  
<http://www.dailynk.com/english/read.php?catId=nk00100&num=6392>.
- Rid, Thomas, and Ben Buchanan. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 4–37. doi:10.1080/01402390.2014.977382.
- Rotella, Sebastian. “Four Disturbing Questions About the Mumbai Terror Attack | American Terrorist | FRONTLINE | PBS,” February 22, 2013.  
<http://www.pbs.org/wgbh/frontline/article/four-disturbing-questions-about-the-mumbai-terror-attack/>.
- Rotella, Sebastian, James Glanz, and David E. Sanger. “In 2008 Mumbai Attacks, Piles of Spy Data, but an Uncompleted Puzzle - ProPublica.” *Pro Publica*, December 21, 2014.  
<https://www.propublica.org/article/mumbai-attack-data-an-uncompleted-puzzle>.
- “Rules and Procedure for the Scientific Advisory Board and Temporary Working Groups of Scientific Experts”. *Organization for the Prohibition of Chemical Weapons*. Accessed May 10, 2017. <https://www.opcw.org/about-opcw/subsidiary-bodies/scientific-advisory-board/rules-of-procedure/>
- “Russian Navy Expert Team’s Analysis on the Cheonan Incident : North Korea : News : The Hankyoreh,” May 2, 2017.  
[http://english.hani.co.kr/arti/english\\_edition/e\\_northkorea/432230.html](http://english.hani.co.kr/arti/english_edition/e_northkorea/432230.html).
- “Sanctions List Materials.” *United Nations Security Council Subsidiary Organs*, n.d.  
[https://www.un.org/sc/suborg/en/sanctions/1267/qa\\_sanctions\\_list](https://www.un.org/sc/suborg/en/sanctions/1267/qa_sanctions_list).
- Sanger, David E., David Bardoza, and Nicole Perlroth. “China’s Army Is Seen as Tied to Hacking Against U.S.” *The New York Times*, February 18, 2013.  
<http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>.
- Schneier, Bruce. “Attack Attribution and Cyber Conflict.” *Schneier On Security*. March 9, 2015. Accessed May 23, 2017.  
[https://www.schneier.com/blog/archives/2015/03/attack\\_attribut\\_1.html](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)

- <http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html>
- Schwartz, Mattathias, "Cyberwar For Sale," *The New York Times Magazine*, January 4, 2017, accessed June 7, 2017, <https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html>.
- "SEC Approves One Watchdog for Brokers Big and Small." Accessed May 2, 2017. [http://www.washingtonpost.com/wp-dyn/content/article/2007/07/27/AR2007072700108\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2007/07/27/AR2007072700108_pf.html).
- "SEC.gov | Hedge Fund Manager to Pay \$44 Million for Illegal Trading in Chinese Bank Stocks," May 2, 2017. <https://www.sec.gov/news/press-release/2012-2012-264htm>.
- "Secretariat and Budget." Annual Report. WTO, 2016. [https://www.wto.org/english/res\\_e/booksp\\_e/anrep\\_e/anrep16\\_chap9\\_e.pdf](https://www.wto.org/english/res_e/booksp_e/anrep_e/anrep16_chap9_e.pdf).
- "Services." *FireEye*. Accessed May 1, 2017. <https://www.fireeye.com/services.html>.
- "Security Council Condemns Attack on Republic of Korea Naval Ship 'Cheonan', Stresses Need to Prevent Further Attacks, Other Hostilities in Region | Meetings Coverage and Press Releases." Accessed May 16, 2017. <https://www.un.org/press/en/2010/sc9975.doc.htm>.
- Shamsi, Jawwad A., Sherali Zeadally, Fareha Sheikh, and Angelyn Flowers. "Attribution in Cyberspace: Techniques and Legal Implications." *Security and Communication Networks* 9 (n.d.): 2886–2900.
- Shukman, David. "Open Sesame: Science Center Unveiled in Jordan." *BBC News*, May 16, 2017, sec. Science & Environment. <http://www.bbc.com/news/science-environment-39927836>.
- "Sinking Report.doc - 20\_05\_10jigreport.pdf," May 2, 2017. [http://news.bbc.co.uk/nol/shared/bsp/hi/pdfs/20\\_05\\_10jigreport.pdf](http://news.bbc.co.uk/nol/shared/bsp/hi/pdfs/20_05_10jigreport.pdf).
- "So How Is Bellingcat Funded?," March 25, 2016. <http://www.whathappenedtoflightmh17.com/so-how-is-bellingcat-funded/>.
- "Sony Hires Mandiant after Cyber Attack, FBI Starts Probe." *Reuters*, December 1, 2014. <http://www.reuters.com/article/us-sony-cybersecurity-mandiant-idUSKCN0JE0YA20141201>.
- "South Korea Warship Sinking: The Top 10 Conspiracy Theories - Telegraph," May 2, 2017. <http://www.telegraph.co.uk/news/worldnews/asia/northkorea/7803376/South-Korea-warship-sinking-the-top-10-conspiracy-theories.html>.
- "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. <http://www.un.org/press/en/2010/sc9923.doc.htm>.
- "Special Verification Commission (INF Treaty) Held 30th Session November 15-16 in Geneva » US Mission Geneva." Accessed April 10, 2017. <https://geneva.usmission.gov/2016/11/18/special-verification-commission-inf-treaty-held-30th-session-november-15-16-in-geneva/>.
- Soldatov, Andrei, and Irina Borogan. "Putin Brings China's Great Firewall to Russia in Cybersecurity Pact." *The Guardian*, November 29, 2016. <https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact>.

- “Statement of Revenue and Expenditure of the European Police Office for the Financial Year 2017.” Office Journal of the European Union.
- “Statement on Google Operations in China.” *U.S. Department of State*, May 2, 2017.
- “Statement to the Board – Nuclear Verification in Iran.” Text, March 3, 2008.  
<https://www.iaea.org/newscenter/multimedia/videos/statement-board-%E2%80%93-nuclear-verification-iran>.
- Stone, Brad and Michael Riley, “Mandiant, the Go-To Security Firm for Cyber-Espionage Attacks.” *Bloomberg*, February 8, 2013. Accessed April 28, 2017.  
<https://www.bloomberg.com/news/articles/2013-02-07/mandiant-the-go-to-security-firm-for-cyber-espionage-attacks>.
- “Structure | CCDCOE.” Accessed May 4, 2017. <https://ccdcoe.org/structure-0.html>.
- “Structure and Organization of the Egmont Group of Financial Intelligence Units - The Egmont Group.” Accessed April 3, 2017. <https://www.egmontgroup.org/en/content/structure-and-organization-egmont-group-financial-intelligence-units>.
- “Structure and People.” *Amnesty International*. Accessed May 1, 2017.  
<https://www.amnesty.org/en/about-us/how-were-run/structure-and-people/>.
- “Suggested Best Practices for Industry Outreach Programs to Stakeholders.” Federal Energy Regulatory Commission, July 2015.  
<https://www.ferc.gov/industries/gas/enviro/guidelines/stakeholder-brochure.pdf>.
- Sullivan, Ben. “Bellingcat Wants Your Help to Debunk Fake News.” *Motherboard*, March 7, 2017. [https://motherboard.vice.com/en\\_us/article/bellingcat-wants-your-help-to-debunk-fake-news](https://motherboard.vice.com/en_us/article/bellingcat-wants-your-help-to-debunk-fake-news).
- “Tallinn Manual Process | CCDCOE.” Accessed May 4, 2017. <https://ccdcoe.org/tallinn-manual.html>.
- “Technology | FINRA.org.” Accessed May 16, 2017. <https://www.finra.org/about/technology>.
- “The 2007 Estonian Cyberattacks: New Frontiers in International Conflict.” *On Cyber Way Harvard Law School Blog*. Accessed May 17, 2017.  
<https://blogs.harvard.edu/cyberwar43z/2012/12/21/estonia-ddos-attackrussian-nationalism/>.
- “The Agency’s Programme and Budget 2016-2017.” IAEA, July 2015.  
[https://www.iaea.org/About/Policy/GC/GC59/GC59Documents/English/gc59-2\\_en.pdf](https://www.iaea.org/About/Policy/GC/GC59/GC59Documents/English/gc59-2_en.pdf).
- “The Egmont Group Strategic Plan 2014 – 2017,” May 2015.  
[https://egmontgroup.org/en/filedepot\\_download/1658/40](https://egmontgroup.org/en/filedepot_download/1658/40).
- “The Sinking of the Cheonan - The New York Times,” May 2, 2017.  
<http://www.nytimes.com/2010/05/21/opinion/21fri2.html>.
- “The Stakes and Challenges of International Civil Aviation.” Montreal: ICAO, February 17, 2011.  
<http://www.icao.int/Newsroom/Speeches/THE%20STAKES%20AND%20CHALLENGES%20OOF%20INTERNATIONAL%20CIVIL%20AVIATION%20-%20Secretary%20General%20Raymond%20Benjamin.pdf>.
- “The U.S.-Israeli Stuxnet Alliance.” *Stratfor*, January 17, 2017.  
<https://www.stratfor.com/analysis/us-israeli-stuxnet-alliance>.
- “Tiger Asia Management, LLC, et Al. (Release No. LR-22569; December 13, 2012),” May 2, 2017.  
<https://www.sec.gov/litigation/litreleases/2012/lr22569.htm>.

Timm, Trevor. "SecureDrop Undergoes Second Security Audit." *Freedom of the Press Foundation*, January 20, 2014. <https://freedom.press/news-advocacy/securedrop-undergoes-second-security-audit/>.

"Treaty Between the United States of America And The Union Of Soviet Socialist Republics on The Elimination of Their Intermediate-Range and Shorter-Range Missiles (INF Treaty)." U.S. Department of State. Accessed May 1, 2017. <https://www.state.gov/t/avc/trty/102360.htm>.

UAE General Civil Aviation Authority. "Gaps in Global Effectiveness." [http://www.icao.int/Meetings/AMC/SAR2010/Documents/21June2010-1030-Brian\\_Day-Gaps\\_in\\_Global\\_Effectiven.pdf](http://www.icao.int/Meetings/AMC/SAR2010/Documents/21June2010-1030-Brian_Day-Gaps_in_Global_Effectiven.pdf).

"Update on Sony Investigation." Press Release. *Federal Bureau of Investigation*. Accessed April 30, 2017. <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>.

"U.S. Hacked into Iran's Critical Civilian Infrastructure for Massive Cyberattack, New Film Claims." *Buzzfeed*, May 16, 2016. [https://www.buzzfeed.com/jamesball/us-hacked-into-irans-critical-civilian-infrastructure-for-ma?utm\\_term=.nxgZMvM1z#.eclLmVmWX](https://www.buzzfeed.com/jamesball/us-hacked-into-irans-critical-civilian-infrastructure-for-ma?utm_term=.nxgZMvM1z#.eclLmVmWX).

"VIENNA DOCUMENT 2011 ON CONFIDENCE-AND SECURITY-BUILDING MEASURES." OSCE. Accessed May 1, 2017. <http://www.osce.org/fsc/86597?download=true>.

"VirusBlokAda." *VirusBlokAda*. Accessed May 1, 2017. <http://anti-virus.by/en/tempo.shtml>.

Walters, Riley. "Cyber Attacks on U.S. Companies Since November 2014." *The Heritage Foundation*. November 18, 2015. Accessed May 23, 2017. <http://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014>.

"War in the Fifth Domain." *The Economist*, July 1, 2010. Accessed May 17, 2017. <http://www.economist.com/node/16478792>.

Warren, Zach. "Are You Ready for the New China Cybersecurity Law?" *Inside Counsel*, February 28, 2017. <http://www.insidecounsel.com/2017/02/28/are-you-ready-for-the-new-china-cybersecurity-law?ref=footer-news>.

Wheeler, David and Gregory Larsen. Institute for Defense Analysis, Techniques for Cyber Attack Attribution ES. October 2003. <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859>.

"Who We Are." *Amnesty International*. Accessed April 29, 2017. <https://www.amnesty.org/en/who-we-are/>.

"Why America Should Keep Supporting the IAEA | The National Interest Blog." Accessed May 4, 2017. <http://nationalinterest.org/blog/the-buzz/why-america-should-keep-supporting-the-iaea-20485>.

"Wilder Security." Wilder Security Forums. Accessed May 1, 2017. <https://www.wilderssecurity.com/threads/son-of-stuxnet.310195/>.

Williamson, Wade. "Lessons from Mandiant's APT1 Report," *SECURITY WEEK*, February 29, 2013. Accessed April 29, 2017, <http://www.securityweek.com/lessons-mandiant%E2%80%99s-apt1-report>.

Wittes, Benjamin, "Mandiant Report on 'APT 1'," *Lawfare.org*, February 20, 2013. Accessed April 29, 2017, <https://lawfareblog.com/mandiant-report-apt1>.

Wolf, Amy F. "Monitoring and Verification in Arms Control." Congressional Research Service, December 23, 2011. <https://fas.org/sgp/crs/nuke/R41201.pdf>.

- “Work and Mandate.” *Security Council Committee Established Pursuant to Resolution 1718 (2006)*, n.d.  
[https://www.un.org/sc/suborg/en/sanctions/1718/panel\\_experts/work\\_mandate](https://www.un.org/sc/suborg/en/sanctions/1718/panel_experts/work_mandate).
- “Work and Mandate.” *United Nations Security Council Subsidiary Organs*, n.d.  
<https://www.un.org/sc/suborg/en/sanctions/1267/monitoring-team/work-and-mandate>.
- “WTO | Budget for the Year 2013.” Accessed May 2, 2017.  
[https://www.wto.org/english/thewto\\_e/secret\\_e/budget\\_e.htm](https://www.wto.org/english/thewto_e/secret_e/budget_e.htm).
- “WTO | Trade and Environment.” Accessed May 2, 2017.  
[https://www.wto.org/english/tratop\\_e/envir\\_e/envt\\_rules\\_exceptions\\_e.htm](https://www.wto.org/english/tratop_e/envir_e/envt_rules_exceptions_e.htm).
- “WTO | Understanding the WTO - A Unique Contribution.” Accessed May 2, 2017.  
[https://www.wto.org/english/thewto\\_e/whatis\\_e/tif\\_e/disp1\\_e.htm](https://www.wto.org/english/thewto_e/whatis_e/tif_e/disp1_e.htm).
- Zetter, Kim. "Blockbuster Worm Aimed for Infrastructure, But No Proof Iran...." *WIRED*, September 23, 2010. Accessed May 23, 2017,  
<https://www.wired.com/2010/09/stuxnet-2/>.
- Zetter, Kim. "Cyberwar Issues Likely to Be Addressed Only After a Catastrophe," *WIRED*, February 17, 2011. Accessed May 23, 2017.  
<https://www.wired.com/threatlevel/2011/02/cyberwar-issues-likely-to-be-addressed-only-after-a-catastrophe>.
- Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *WIRED*. July 11, 2011. Accessed May 24, 2017.  
<https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/>.
- Zheng, Denise, and James Lewis. "Cyber Threat Information Sharing." *Center for Strategic and International Studies*, March 10, 2015. Accessed May 17, 2017.  
<https://www.csis.org/analysis/cyber-threat-information-sharing>.