CSAW'21 Policy Competition

Background Paper for Cyber Attributions

General Background

Over the past decade, publicly attributing cybercrime to specific state and private actors has become more common and less difficult to achieve than many believed in the early 2000's. In 2020, cyberattacks cost global governments and businesses almost 1 trillion dollars.[i] The growing capability to make attributions along with the increasing damage from cyber incidents has spurred increased study into public and private sector attribution.

For this competition, this topic area will not address the specific technical procedures or tools used in network analysis. Instead, the focus is on the political aspects of "a specific adversary as the ultimately responsible party",[ii] and untangling the policy challenges related to attribution and accountability.

Public-Sector Attribution

Historically, governments retained a monopoly on attribution, linking hostile actions with foreign or domestic adversaries.[iii] Along with the rise of private-sector attribution, the anonymity of cyberspace, nascent cyber norms regimes, and blurring of State and non-State actors has made the attribution of cybersecurity incidents especially difficult for governments to adapt to.

The choice to make a public attribution is a political decision that rests with a country's executive, but the abilities for governments to make attributions are not the same. The Five Eyes alliance has the capabilities to collect, analyze, and internally-share information leading to high-confidence attributions; however, many of the sources and processes cannot be shared with the public to protect their integrity. On the other extreme are countries without an infrastructure or workforce to monitor, protect, and defend their networks, much else attribute activities to other nation-state or private actors.

Private-Sector Attribution

One of the first extensive cyber attributions was not made by a government, but by a private company. In 2013, private cybersecurity firm Mandiant released a 76-page investigation report accusing Unit 61398 of the Chinese army of cyber espionage. In 2014, the US government charged five members of Unit 61398 after concluding its own investigation. [iv]

This year-long difference in attributing the same group implies several key differences with private sector attributions, such as faster response and more detailed investigation reports because there is no declassification process. Additionally, private industry has a range of stakeholders both foreign and domestic and market incentives to make attributions quickly. These diverse motivations make the credibility of private sector attributions questionable.

Though governments may have information well-ahead of private companies, they must go through lengthy processes weighing the benefits and risks of sharing information publicly. As with the Mandiant case-study, it is unclear if prior private-sector attributions can spur or assist governmental attributions.

Main Issues

Competitors must choose **one** subtopic. They must address **at least one** bullet point within that subtopic as listed below.

Subtopic A: Public-Sector Attribution

- Global evidentiary standards for governmental, political cyber attributions
- Making attributions more effective as part of a deterrence strategy
- Using existing international bodies in the attribution process

Subtopic B: Private-Sector Attribution

- Creating common attribution evidentiary standards for threat intelligence firms
- Protections for companies after making false or unflattering attributions
- Standards for governments' use of private sector attribution in official accusations
- Privacy protections for private-sector organizations in collecting on which technical attribution relies

What needs to be covered

Between competitor's Policy Brief and Presentation, all of the bullet points below **must** be addressed.

- **Public-Private Cooperation:** How does your policy incentivize private sector cooperation? What weight should be accorded to private sector considerations during strategic decision making?
- **International Diplomacy & Law:** How does your policy utilize existing international organizations, intraregional legal regimes, and diplomatic efforts to accomplish its objectives? Does your policy require close cooperation with regional stakeholders? If current laws/organizations are inadequate, what changes are required in order to facilitate cooperation?
- **Short & Long-Term Goals:** What is the timeframe for your policy? How does your policy assess short- and long-term success in accomplishing its objectives?

A note to CSAW Competitors

This brief is a starting point for your policies and ideas. It contains things you must address, but scope, definitions, and specific content will come from you. We encourage bold, creative policies that force deep thought and discussion. Leaders from academia, government, and private industry may see your work, and thus we encourage you to prioritize your policies by thinking through their practicality and implementation for a range of stakeholders. Please reach out to the CSAW committee at csaw-policy@nyu.edu with any questions.

Endnotes and Useful References

i. Riley, Tonya. “The Cybersecurity 202: Global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report finds.” *The Washington Post*, December 7, 2020. https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/.

ii. Knake, Robert K. “Untangling Attribution: Moving to Accountability in Cyberspace.” *Council on Foreign Relations*, July 15, 2010. https://www.cfr.org/sites/default/files/pdf/2010/07/Knake%20-Testimony%20071510.pdf.

iii. Lin, Herbert. “Attribution of Malicious Cyber Incidents: From Soup to Nuts.” *Columbia Journal of International Affairs*, September 2, 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2835719.

iv. Eichensehr, Kristen E. “Symposium On Cyber Attribution: Decentralized Cyberattack Attribution.” The American Journal of International Law; AJIL Unbound 113. 2019. https://doi.org/10.1017.

Clark and Susan Landau." National Research Council. 2010. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. 25-40.

Detlefson, MAJ William. “Cyber Attacks, Attribution, and Deterrence: Three Case Studies.” *United States Army Command and General Staff College*, 2015. https://apps.dtic.mil/sti/pdfs/AD1001276.pdf.

Eichensehr, Kristen E. “The Law of Politics of Cyberattack Attribution.” *University of California, Los Angeles*, September 15, 2019. http://www.med.a51.nl/sites/default/files/pdf/SSRN-id3453804.pdf.

Healey, Jason. “The Spectrum of National Responsibility for Cyberattacks.” The Brown Journal of World Affairs 18, no. 1 (2011): 57–70.

Romanosky, Sasha and Benjamin Boudreaux. “Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government.” *International Journal of Intelligence and Counterintelligence*, September 1, 2020. https://www.rand.org/pubs/external_publications/EP68257.html.

Tatar, Unal, Brian Nussbaum, Yasir Gokce, and Omer F. Keskin. “Digital force majeure: The Mondelez case, insurance, and the (un)certainty of attribution in cyberattacks.” *Business Horizons*, July 31, 2021. https://www.sciencedirect.com/science/article/pii/S0007681321001361?via%3Dihub.

Yannakogeorgos, Panayotis A. “Strategies for Resolving the Cyber Attribution Challenge:” Fort Belvoir, VA: Defense Technical Information Center, May 1, 2013. https://doi.org/10.21236/ADA602150.

By: Amanda Tobey, Liao Hu, Ricky DeMello