Unlearned Lessons Behind Building a Shared Cyber Framework

with your Geo-Political Adversaries – the Hacker Perspective

Chris Spirito

Even in times of seemingly intractable geo-political conflict, geo-political competitors can find opportunities to develop a common cyber framework – the "Shared Cyber Framework." Achieving cyber stability between two or more nations is not predicated on congruence across all domains of cyber engagement, nor can silence among adversaries advance international stability. From a hacker perspective, this observation seems obvious. Indeed, the technical exchanges during the Cold War between the United States (US) and the former Soviet Union are said to have measurably contributed to both the stability of the bipolar world and, ultimately, the end of the conflict.[1] Yet the current generation of leaders in the major cyber powers have neglected this lesson, both those who exploit access to westernized technologies and those who have responded by attempting to freeze out the attacking nation. For the past few years, the US and China, for example, have increasingly withdrawn from fruitful bilateral discussions. The January 2021 revelations of the Chinese Hafnium Zero Day hack riding shotgun after the December 2020 Russian SolarWinds campaign discoveries suggest few major cyber powers have progressed in finding even small areas of agreement on which to build confidence and a common framework.

Without the lessons that can be learned from common efforts, building spaces in which other areas of contention can be worked to improve stability and peace will be quite difficult. In the hacker community, there is very little trust and yet groups find ways to collaborate in exploits, campaigns, and even distribution of rewards. Using primarily

Chris Spirito is a Nuclear Cyber Security Analyst for Idaho National Laboratory (INL). He supports Nuclear-Cyber work programs with US partners and is PI for a research program on remote and autonomous operations for advanced reactors. Prior to joining INL, Chris was the International Cyber Lead for The MITRE Corporation. He is also a board member for WiRED International, a global health NGO providing medical education to underserved regions of the world.

Title: Nuclear Cyber Security Analyst

Affiliation: Idaho National Laboratory

Academic Background: Boston College, Harvard School of Public Health, Worcester Polytechnic Institute

the author's experiences in cross-adversary efforts to secure nuclear power plants from cyber-attacks, the following essay identifies axioms for collectively advancing ideas for cooperation, despite wider state-state distrust, and for creating from the bottom up a Shared Cyber Framework.

Find a common problem to work on together in safe domains

When the problem space includes the whole gamut of geo-political conflict, one should avoid domains where the equity dynamics are too fluid to control. What might be common interests in the military and intelligence problem spaces can be immediately excluded, along with international monetary systems and, apparently, pandemic response. Each of these domains is deeply affected by cyber-security architectural dependencies as well as cyber-defensive mechanisms used as a response to hostile actions. Learning the lesson means identifying a domain where both (all) parties are invested in operational success and overtly agree that operational failures would be destabilizing, at a minimum, to their own society, and possibly more broadly destabilizing to the global community and earth's ecosystem.

For example, one area of common interest for geo-political adversaries would be the safe operation of nuclear power plants and research reactors. The horrific impact from a dirty bomb created using stolen nuclear material, or a core meltdown within a nuclear reactor, is almost universally recognized and thus provides a pathway for major powers' engagement. One advantage of this problem space is that, at least in this case, the problems and solutions are not limited to the geo-political rivals, as they extend to all nuclear regimes, and thus there exist engagement pathways with the possibility of many trusted intermediaries.[2]

Leave nationalist ideology at the door

Ideology influences international relations throughout history. Diplomatic relations are shaped by these ideologies, but often these perceptions and judgments instantiated by diplomats become roadblocks to cooperation. Using a bottom-up approach, engineers, scientists, and field technicians can more easily leave their ideology outside the door, and more readily identify their technically trained counterparts able to focus on the common problem and use that joint effort as a platform for confidence building. This advantage was particularly evident during the Cold War technical exchanges.[3]

It does require considerable dissociation at times to rationalize working with citizens of nations whose leadership engages in less than savory actions from targeted assassinations of their citizens to destabilizing critical infrastructure of neighbors due to perceived injury over fallen statues. However, the bottom-up approach allows for targeted engagement[4] and narrow problem-bounded confidence building with the goal of deceasing risk in the problem space and offers an alternative and usable channel for crisis management and de-escalation in the face of cyber campaigns. This approach also allows the diplomatic engagement tied to the technological exchanges to avoid fractious ideological space since, in most instances, mild norms-violating behavior by engineers and scientists can be disavowed from above.

Create a reciprocal immersive cultural exchange

Once a team is in place, invest in reciprocal immersive cultural exchange with the goals of creating deeper emotional connections between counterparts and improving analytical conclusions that seek to represent counterpart positions. Decision paralysis or less-than-optimal engagement pathways are often the result of misreading both event interpretation and reaction options. This is also a cycle that feeds on itself and requires a special type of lateral thinking and ideological mushiness. Examples of this would be the Soviet submariner Vasili Arkhipov, who is credited with preventing a nuclear strike during the Cuban Missile Crisis (strategic lateral thinking) and more broadly, misperceptions by every country that the US is a streamlined bureaucracy adept at centralized planning and coordination. We need this immersive cultural exchange to provide environmental perspective and develop an intimacy with our counterparts to better see the world through their eyes.

> It is intimacy that is supposed to give us a glimpse of different points of view – we might not become the people we study, but by living, thinking, and feeling close to them we should be able to understand how they see the world.[6]

These types of cultural exchanges are not difficult for those open to the experience. In the US these activities have taken the form of foreign technical teams visiting gun ranges and National Parks along with partaking in local culinary treats, such as New Jersey Pork Rolls.

In other countries, as this author has experienced, these cultural exchanges could include more exotic experiences. In the cybered world, critical information about vulnerabilities is not generally shared between organizations; it is shared between people speaking with each other, usually face to face. Requests for assistance in the face of cyber campaign surprises requires trust built on this cross-team intimacy, plus a healthy amount of cognitive dissonance on occasion.

Analyze and Prepare for Political Interference early on

If isolated from wider conflicts, technical team members can focus on solving problems together. The joint focus and associated interpersonal intimacy allow freedom of communication and a generally less bounded information-sharing space. However, the cyber domain is not immune from competing interests. It is important to decide from the outset how team members will handle types of political intrusions. For example, one could be making progress on better protecting a 'Nuclear Reactor Protection System' (RPS) from cyber-attacks and suddenly find oneself being approached in the off-hours with a request that the progress be slowed down. Or, if slowing the results is not possible, then a request for more information on how those new protection mechanisms can be subverted. It is essential to have each team evaluate what equities they will value in efforts to compromise the project, and that they be equipped with analysis and remediation skills. Deconfliction pathways need to be identified and made available in advance.[7]

This requirement is particularly complex and important when counterparts are not citizens of a nation that values free speech and face the possibility that they and their families could face physical harm if they refuse to compromise the project. For example, some signaling options that can established, such as an adaptation of a "warrant canary"[8] to indicate that a partner's freedom of movement and speech have been limited in some way. Reporting political interference through counterintelligence channels may serve as a deterrent as well as leveraging official diplomatic channels to make other parties aware of these destabilizing behaviors. How these actions are authorized and carried out in each country should be documented when identified and shared to maintain a working level of trust that lowers overall risk of disrupted engagement.

Exercise alternative Crisis Management protocols often

There was an elaborate telex connection installed after the Cuban Missile Crisis to link the president of the United States with the party secretary of the Soviet Union so that future crises could be resolved without nuclear exchanges.[9] In 2013 the Moscow-Washington Cyber Hotline was established, and affectionately called the "Red Phone".[10] President Obama used it once to warn Russia about interference in the 2016 election.[11] The difficulty is that such crisis communications devices are used so infrequently that reciprocal exchanges to build trust do not occur. The cyber hotline was established but did not demonstrably allay concerns about preventing a cyber war from breaking out.

In the same way that political intrusions should be prepared for, exercising crisis management channels and protocols is necessary from the outset. One scenario that could be used is discovery of an implant within the shared domain, such as a piece of malware on an RPS, and what the escalation pathways would look like before and after applying this deconfliction channel. This scenario would be exercised from both (all) participants' perspectives, and stakeholders would be included depending upon which de-confliction channels and processes they want to see exercised.

If a bottom-up approach—identifying a common problem to work on, engaging in reciprocal immersive cultural exchanges, and deconflicting political intrusions—is strategically employed from the outset, there is a greater chance that trusted communication channels will exist and can be expanded to include crisis management if necessary. The success of this model also depends upon each participant having developed a commensurate reputation for trustworthiness within their own national infrastructure. To the extent that they are perceived as trusted resources within the crisis management process, their perspectives aid in deconflicting misperceptions and accurately representing response options and the spectrum of counter-responses across states. Increased transparency provided through a trusted channel will help de-escalate responses in a measured way. Furthermore, this determined but incremental approach would also be welcome so that any sensitive incident response processes and procedures can be offered in a gated progression avoiding instability.

CONCLUSION

Today there is no Shared Cyber Framework among the major geo-political adversaries. There does not exist the typical industrial or even hacker group cooperation among cyber domain participants. Thus, the channels that are available in other domains to facilitate crisis de-escalation are at best anemic. The risk of escalation is greater since the rules of crisis management and behavior are not agreed upon and governing relationships among adversary nations as complementary or at least acceptably global competition. To address this challenge, nations need to find a common interest problem to work on together within the cyber domain, and then engage in confidence-building measures such as reciprocal immersive cultural technological exchanges built with the recognition of ideological boundary conditions and how they need to evolve over the course of the relationship. The engagement risk will be contained if the domains chosen for the common problem-solving efforts are not overly contested. The probability of success will likely also be heavily influenced by the individuals chosen by each participating nation and the support provided – especially in avoiding political interference – as the relationship grows. In short, this bottom-up approach so present in the Cold War needs to be a lesson relearned. With patience, measured achievements in shared cybersecurity can be realized.

NOTES

1. Olga Krasnyak, "How US-Soviet Scientific and Technical Exchanges Helped End the Cold War," *American Diplomacy* (2019).
2. Do-Yeon Kim, "Cyber security issues imposed on nuclear power plants," *Annals of Nuclear Energy* 65 (2014).
3. Olga Krasnyak, "The Apollo–Soyuz Test Project: Construction of an Ideal Type of Science Diplomacy," *The Hague Journal of Diplomacy* 13, no. 4 (2018).
4. V. Levitov and H. Long, "US-USSR cooperation in superconducting power transmission," *IEEE Transactions on Magnetics* 15, no. 1 (1979).
5. Jervis, Robert. *Perception and Misperception in International Politics: New Edition*. REV - Revised ed., Princeton University Press, 1976. JSTOR, www.jstor.org/stable/j.ctvc77bx3. Accessed 16 Mar. 2021.
6. Katarina Kušić and Jakub Záhora, Fieldwork, Failure, International Relations, E-International Relations, 2020, https://www.e-ir.info/2020/03/30/fieldwork-failure-international-relations, accessed March 16, 2021.
7. Arian L. Pregenzer, *Learning from the Past and Challenges for the Future: The Role of International Technical Cooperation*, Sandia National Lab (SNL-NM), Albuquerque, NM (2011).
8. Rebecca Wexler, "Warrant canaries and disclosure by design: The real threat to National Security Letter gag orders," *Yale LJF* 124 (2014).
9. Tobias Nanz, "Communication in Crisis. The" Red Phone" and the" Hotline"," *BEHEMOTH-A Journal on Civilisation* 3, no. 2 (2010).
10. Andrew Futter, *What Does Cyber Arms Control Look Like?: Four Principles for Managing Cyber Risk* (European Leadership Network., 2020).
11. Erica D. Borghard and Shawn W. Lonergan, "Confidence building measures for the cyber domain," *Strategic Studies Quarterly* 12, no. 3, (2018).