Shining a Light on Cyber

An Interview with John C. "Chris" Inglis

Former Deputy Director, National Security Agency
Member, Cyberspace Solarium Commission

Conducted 4 July 2020

The Cyberspace Solarium Commission was established through the 2019 National Defense Authorization Act (NDAA) and charged with answering two questions: "What strategic approach will defend the United States against cyberattacks of strategic consequence? And what policies and legislation are required to implement that strategy?" The Commission began in the spring of 2019 and included four legislators; the deputies of the Departments of Defense, Justice, and Homeland Security; the director of national intelligence; and six commissioners appointed from the private sector by the majority and minority leaders of the House and Senate. It conducted over 300 engagements across the private and public sectors, including 30 face-to-face Commission meetings. The Commission report of 11 March 2020 recommended an overall strategy along with 82 proposals centered around six key areas: government organizational reform, international norms, national resilience, reshaping the cyber system, private-sector collaboration, and the military instrument of power. The entire report can be found at https://www.solarium.gov/. This interview with commissioner Chris Inglis is a behind-the-scenes view of cybersecurity and the Commission's work.

***SSQ*: How bad is the threat to our national security, and is the threat worse in one area, such as infrastructure or commerce?**

JCI: The digital era has brought economic growth, technological innovation, and an improved quality of life to nearly every American. It has also created a strategic dilemma. The more digital connections we make and data we exchange, the more opportunities adversaries from criminals to nation-states have to intrude on national defense, disrupt critical functions, and damage our economic and democratic institutions. The Solarium Commission worked over the past year to identify and address several key national security problem areas, including the defense of our critical infrastructure.

First and foremost, our nation lacks an integrated national cyber strategy. There are inconsistencies and gaps across the various departments and agencies, and our nation does not have a cohesive vision for how to work together across the federal enterprise, let alone with the private sector. Second, most of our critical infrastructure is owned and operated by

the private sector and faces increasing attacks by malicious cyber actors on a daily basis, to include adversarial nation-states. And while the skirmish lines of cyberspace are quite literally manned by the private sector, the government can and must do more to support its efforts with a robust, proactive, and collaborative application of the full suite of government-unique authorities and capability. Third, we must get faster and smarter, improving the government's ability to organize concurrent, continuous, and inherently collaborative initiatives to build resilience, respond to cyber threats, and preserve whole-of-government options that signal capability and willingness to impose costs on adversaries.

***SSQ*: The report critiques current US organization and structure for cyber as inadequate and proposes a new national cyber director, but it does not recommend eliminating any of the current competing organizations. Why not?**

JCI: The Commission determined that the fundamental problem across the federal cyber enterprise was a lack of coherence—not duplicative efforts or competition—a problem significantly exacerbated by the lack of a person or organization accountable for anticipating and preparing for coordinated action. Looking at the history and current structure of the executive branch, three clear institutional challenges emerged. First, the federal government lacks consistent, institutionalized leadership in the White House on cyber and cybersecurity. Second, due to the lack of a consistent advocate, cybersecurity is inconsistently prioritized in the context of national security. Third, the United States lacks a coordinated, cohesive, and clear strategic vision for cyber. While a national-level cyber coordination position has existed in various forms within the White House through the years, it has never been Senate confirmed. It also inherently did not have a robust ability to influence the president's budget or to convene decision makers to prepare and recommend a coordinated strategy and lines of effort to the president. In considering how best to implement such a role, we did not find any organization currently assigned to it, leading us to conclude that we needed to create the role rather than eliminate one or more of the stovepipes.

***SSQ*: The tone of the recommendations appears quite aggressive. Is this an accurate description, and was this the intent?**

JCI: The report and its recommendations *are* aggressive, but it is important to note their overwhelming focus on defense and deterrence. It is past time for the US to seize the initiative ceded to adversaries by our collective

failure to increase the cost of their aggression as a deterrent to their further escalation. The central message embedded in the Commission's recommended strategy is that the US intends to undercut the advantage adversaries have enjoyed in being able to selectively target and defeat weak links in our system. Henceforth, an adversary will find the US more resilient, unified, capable, and willing to impose costs for bad behavior. The Commission's recommended strategy is therefore one of "layered cyber deterrence" based on investments in norms, resilience, proactive defense, cost imposition, a more robust public-private partnership, and leverage accruing from international coalitions.

The Commission recognized the strategic merits of the Defense Department's "defend forward" 2018 cyber strategy. At its heart, defend forward is about protecting the things the United States holds dear, like its democratic institutions, economy, and way of life.

The concept of forward defense has long-standing historical roots. American grand strategy during the Cold War was anchored in this concept. Moreover, there are also risks associated with inaction or, worse, tolerating bad behavior. Defend forward will include taking actions at the operational and tactical levels that will change how our adversaries understand our priorities and decision calculus and, in turn, choose to operate in the domain. We also have to be more proactive in communicating the United States' intentions, goals, and means. This is why signaling is so important and why we need a more robust signaling strategy. We can better manage any potential escalation risks that may arise and better communicate with adversaries as well as our allies. In all of this, the Commission deliberately took into account potential escalation risks.

Some reviewers have raised concerns that the Commission's affirmation of the defend forward concept suggests the United States become more offensive in its defense of cyberspace. We wanted to make clear that, in keeping with the defend forward concept as understood by both the Commission and the Department of Defense, it is an inherently defensive strategy that incorporates early warning and early action against material threats to US interests. More importantly, the Commission recommends that the US extend the concept to the use of all instruments of national power, applying legal, diplomatic, and financial tools in a coordinated fashion that adheres to international law and the associated standards of necessity and proportionality.

***SSQ*: Is it probable that democracies may be able to counter what appears to be authoritarian regime advantage in cyberspace?**

JCI: Authoritarian regimes certainly have undeniable advantages in cyberspace. They can subordinate individual citizen interests to those of the state and are better positioned to present a unified front, long term, in various international fora that determine the internet's norms, standards, and protocols. However, the authoritarian approach stifles innovation—which remains the vital engine on which cyberspace continues to be built—and brings with it unacceptable restrictions on human rights along with the imposition of state surveillance and control. The Commission recommends that the United States work with like-minded countries to counter the malicious actions of authoritarian regimes by building on the vitality and innovation delivered by free, open, diverse, and democratic societies while creating coalitions that act in concert to detect, respond to, and punish bad behavior. In the end, we are more likely to be an attractive alternative to nonaligned states by delivering better performance alongside the values America, its partners, and allies hold dear.

***SSQ*: Can cybersecurity norms realistically prevent malicious activities when many offensive cyber operations seem to violate norms?**

JCI: Norms in and of themselves do not prevent malicious activities, but they are the vital foundation on which incentives and consequences affecting human and nation-state behavior must reside. The Commission's proposed deterrence strategy depends on the concurrent and integrated application of three lines of effort: *shaping behavior* by working with the private sector, partners, and allies to define and promote responsible behavior; *denying benefits* to adversaries who would violate accepted rules of behavior; and *imposing costs* on those who do. The ultimate targets of deterrence then are the humans who—singly or collectively—promote, tolerate, or undertake malicious action in cyberspace. They will respond to incentives and consequences if we are clear in articulating them, unified in applying them, and diligent in following through on "promises made" in the form of incentives or cost imposition. Authoritarian regimes, like China and Russia, sometimes have tactical advantage in cyberspace as they violate international norms through operations that disregard agreed rule of law and impinge on human rights. But international norms implemented and reinforced by a coalition of states willing to call out and impose costs for transgressions will affect the decision calculus and ultimately the behavior of rogue actors. This is why the Commission recommends creating and appropriately funding a new Cyberspace Security and Emerging Technologies Bureau led by a new assistant secretary at the Department of State. The assistant secre-

tary will be responsible for coordinating engagements with partners and allies to build and support that coalition.

***SSQ*: Are you concerned about the intersection and comingling of technologies such as cyber, artificial intelligence, quantum computing, and space?**

JCI: The Commission recognizes that emerging technologies such as artificial intelligence and quantum information science pose both opportunities and risks. Several of our recommendations touch on this very issue. More importantly, the Commission recommends that the national cyber director take on the additional responsibility for coordinating federal efforts to anticipate and address emerging technologies. The Commission's report contains specific recommendations that address federal research and development funding levels, quantum computing, related funding support for the National Institute of Standards and Technology (NIST), and support for the President's National Security Telecommunications Advisory Committee (NSTAC) cyber "moonshot" initiative. This initiative recommends a transformative effort to reengineer the underpinnings of cyberspace to yield an inherently more robust, resilient, and defensible domain.

***SSQ*: What's the best way to get the private sector to take cybersecurity seriously?**

JCI: Many in the private sector *do* take cybersecurity seriously and make the types of investments necessary to secure their networks. Clearly some *do not*. The Commission's recommendations offer a mix of incentives, accountability, and consequences to significantly improve the mobilization and commitment of private-sector capabilities needed to create and defend digital infrastructure largely owned and operated by the private sector. While the Commission's recommendations display a preference for the use of market forces and incentives, they also include compulsory action when and where necessary by private- and public-sector entities.

However, mobilizing the stakeholders in cyberspace within their respective silos is at once necessary and insufficient. A private company acting alone will be unable to prevent all breaches and successfully defend against a well-resourced, sophisticated nation-state adversary. The government must also become a valued partner in the defense of cyberspace, employing the full range of its intelligence assets and inherently governmental powers in a mutually beneficial collaboration with the private sector. The US government can thus play a powerful role, supplying companies with threat information that heightens awareness and advances

security without raising private-sector costs and applying the full power of the government to a whole-of-society effort alongside the private sector. To be clear, the government will not patrol and defend private-sector networks, but it can and must stand alongside, and sometimes out in front of, private-sector defenders in a full-throated collaboration

To advance collaboration, the Commission's recommendations focus on expanding and increasing private-sector participation in voluntary threat detection programs, creating a "joint collaborative environment" between the public and private sectors, and working with the federal government to "strengthen and codify processes for identifying broader private-sector cybersecurity intelligence needs and priorities." Where a given sector's criticality and/or risk was deemed to be particularly significant, the Commission provided more specific and tailored recommendations. One example is the US defense industrial base that the Commission recommends should participate in a significantly improved threat intelligence sharing program with the US government and increase threat hunting on its owned networks.

***SSQ*: The Commission proposed that the US observe, pursue, and counter adversaries short of armed conflict. Where is the line? How do we stay below the line, and under what circumstances should the US consider (and signal) our clear intent to cross the line?**

JCI: The specific definition of *what* would constitute the line to be crossed or what would rise to the level of armed conflict remains an inherently political decision. The Commission believes this should continue to be the case in cyberspace as well. The United States can and must clearly signal the kinds of unacceptable activities that would trigger such thresholds, but without constraining the ability of political leaders to maneuver and adapt in the midst of a crisis. To change adversaries' behavior, it isn't sufficient to simply detect and react by only responding to their initiatives, countering their campaigns, and imposing costs. Rather, the United States must signal capability and resolve, as well as communicate the changes it seeks in adversary behavior, to shape the strategic environment. Beyond deterrence, signaling is also essential for escalation management so actions are not unintentionally perceived as escalatory. This is why the Commission recommends a multitiered signaling strategy aimed at altering adversaries' decision calculus and addressing risks of escalation. It is multitiered because it includes signaling mechanisms at the strategic level through traditional channels as well as signaling at the tactical and operational levels through overt and covert means.

***SSQ*: The report states that the public and private sectors should be allowed to defend themselves and strike back. However, it does not address changes to the Computer Fraud and Abuse Act (CFAA). Is this a problem? And what are the implications of hack back?**

JCI: The Commission does not envision or recommend that the private sector engage in "hack-back" activities. We find them to be ineffective and ill advised when applied by organizations lacking the ability to ensure that cyber response actions are coordinated with other government tools (legal, financial, intelligence, and diplomacy key among them) and, as your question notes, the ability to be consistent with US and international law. However, the Commission does recommend the concurrent and coordinated application of all private- and public-sector capabilities and authorities. It moves away from a division of effort between the private and public sectors toward a robust collaboration. It also acknowledges that cyber defense will always have a significant dependency on the underlying efforts of the owners and operators of private networks and infrastructure operating under current authority to prepare and defend their digital infrastructure.

***SSQ*: Can you foresee the prospect of cyber as an existential threat, and if so, how might this occur?**

JCI: Considering the issue of a catastrophic cyberattack, it is important to acknowledge the millions of daily intrusions that disrupt everything from financial transactions to the inner workings of our electoral system. When viewed through that lens, we experience a cyber Pearl Harbor every day. It is just not registered as a shared event in the collective consciousness of the American people. This steady erosion of cyber system integrity married with increasingly bold adversary behavior sets up an increasing possibility of a catastrophic event. As noted throughout the report, critical functions underpinning commerce, travel, health, and safety rely on networks of digital devices. A major cyberattack on our nation's critical infrastructure mounted by a nation-state adversary capable of preparing and sustaining a dedicated campaign would create chaos and lasting damage. The United States can do much to reduce the risk of major attacks through improving deterrence, resilience, and response. The Commission's 82 recommendations offer a strategy and blueprint to mobilize all available resources and authorities to better defend the US in cyberspace and against destructive cyberattacks.

***SSQ*: The report laments that it was not able to solve all the challenges. What were some of those you would have liked to solve? Which solutions required too great a compromise?**

JCI: While we discussed the challenge of aligning various national perspectives on the use of encryption, we did not come to a consensus. While encryption is an essential tool for the protection of the foundations of critical functions in cyberspace, it is also a tool used by some to hide their depredations from legitimate law enforcement. This remains a critical issue on which we wish we could have done more work.

***SSQ*: What do you imagine as the best-case scenario from the Commission's work, and what is the worst-case outcome?**

JCI: The Commission recommended 82 actions with specific outcomes, timelines, and action owners. Of these, 57 require legislative action, and the Commission drafted proposed legislation for consideration by a specific committee of jurisdiction. With that preparatory work in hand, the best case is that the 25 nonlegislative proposals will be broadly adopted by the executive branch and the private sector at whom they are aimed. Additionally, a substantial portion (50 percent or more) of the Commission's legislative proposals would be adopted within the 2021 National Defense Authorization Act or other legislative vehicles over the next six to 18 months. Legislative proposals not adopted in the present Congress have enduring value as "break glass" proposals that remain at the ready for implementation when political will and the conditions of cyberspace align.

The worst case is that the Commission's recommendations join those of other previous commissions already on the shelf, and the nation carries on toward a sure and certain crisis in cyber for which we could have prepared—but failed to do.

***SSQ*: Do you believe this Commission's recommendations will make a difference? If so, how will you know?**

JCI: I do think they will make a difference. Within 90 days following the Commission's report, 11 of our proposals were included in the Senate markup of the NDAA. These will help shore up the military instruments of power—a key pillar in our report. We have hosted or participated in dozens of sessions engaging a diverse array of private-sector, think tank, and government leaders whose efforts will determine the success or failure of the remainder of the Commission's recommended strategy. The reviews and promise of support have been solid at every turn, though the proof will be in the execution. We anticipate that many more of our recommen-

dations will be enacted by Congress or taken up as a shared effort by government and private industry. This will lead to renewed engagement in cybersecurity thinking and planning.

The Senate and the House are currently working to extend the Commission, with a smaller footprint, for another year through the NDAA. We will use that opportunity to continue to facilitate implementation using an assessment tool that will track progress and hone the Commission's body of work through the production of white papers on specific topics of interest. Cyber workforce development is but one example.

SSQ: On behalf of Team *SSQ* and the *SSQ* audience, thank you Mr. Inglis for serving on the Solarium Commission and for sharing your insights on what may well be the most difficult security challenge of the twenty-first century. SSQ