Panel 6: Cyber Security Awareness and Norm-development: Practical issues for Engaging Critical Private Actors

Chris Demchak (chris.demchak@usnwc.edu), US Naval War College,[1] chair and rapporteur
Andrew Cushman, Microsoft;
Sandro Gaycken, Freie Universität Berlin & IT Policy Planner at Federal Foreign Office of Germany
Greg Rattray, Delta Risk LLC
Rafal Rohozinski, SecDev Group
Bill S, senior cyber advisor
Mark Matz, Director of Cyber Policy for Canada's Dept. of Public Safety, discussant

Panel Description

Given the massive role played by private firms in most westernized democracies' national critical infrastructures, it is more effective for any nation's resilience and socio- technical-economic long-term wellbeing if these key private actors voluntarily and collectively collaborate with governments to ensure the whole system's cyber security. In today's highly integrated nation and globe, actions taken locally across critical infrastructure industries, IT capital goods firms, and the mass of cyber victim corporations change the cyber security profiles and systemic wellbeing prospects of societies.

This panel explored objectives for national governments to effectively engage private actors in successful collective and broadly systemic efforts to ensure cyber security for the wider nation. With this engagement over time and across interconnected socio-cyber-economic systems, shared daily practices across the full range of key private and public institutions will induce and embed behavioral expectations, adaptive controls, and, eventually, sustaining norms for future actions. With all communities collectively maintaining situational awareness and preparing for rapid effective actions in the face of disabling cyber surprise and/or systemic enfeeblement, for any nation, the fully digitized future for nations and the international system can be more stable, more secure, and less conflictual.

To that end, the panel members considered the following parametric questions to identify incentives, disincentives, and possible paths forward to engage the private sector communities in national cyber security:

- **Framing:** *How can the C-suite and top managers of businesses in critical infrastructure*

[1] The views expressed in this document are the views of the authors and not the official views of the US government or any of its agencies, of the Federal Republic of Germany or any of its agencies, or the Government of Canada or any of its agencies.

and strategic economic sectors be motivated to respond to critical national security challenges?

- **Analyzing:** *How can enterprise cyber security be reformulated as a value proposition for customers and a profit center for firms, which enhances return on investment?*
- **Instantiating:** *What technology changes are necessary to enable firms to better defend their operations and intellectual property with positive side effects of enhancing national resilience?*
- **Monitoring:** *What innovative approaches can help forge effective public-private partnerships to overcome the cyber defense public goods dilemmas?*
- **Consequence Recognition:** *How can national progress be measured for reducing systemic cyber risk, enhancing cyber resilience, or mitigating strategic economic losses?*
- **Actions:** *In what programs could democracies internally and externally employ distribute fairly and effectively the burden of systemically ensuring cyber security for themselves and their wider community of like-minded nations?*

Panel Findings

Through their individual contributions and collective refinement of ideas, the panel of international subject matter experts broadly converged on three key themes for urgent government action, captured in summary by the labels - motivations, metrics, and (knowledge sharing) structures.

Motivations

Motivating private enterprise cooperation to ensure systemic national cyber resilience requires adjustments in the economic sector's own net assessments of profit, regulations, and traditional business model's treatment of externalities and anticipatory loss leading activities. Across the three main groups of private enterprises determining national cyber wellbeing (critical infrastructure industries, IT capital goods firms, and cyber victim corporations)[2], these elements

[2] John Mallery, Research Scientist at MIT, is thanked for this set of categories. Personal conversation, 2012.

carry different weights in changing motivations for their wider community requiring different approaches to motivate cooperative actions for national cyber security.

Profit is a key motivator for all the firms and must be understood differentially across these three communities. For the critical infrastructure services (CIS) community, profit and regulations are orthogonal. For these firms, their business models accept regulations on allowable costs, calculations of customer fairness, service responsiveness, etc.,as baseline business system constraints on top of which profit (or net assets in nonprofit organizations) are counted. For both the IT capital goods firms and the vast community of cyber victim corporations, however, profit and regulations are viewed as inversely related, with more regulations presumed to directly impair profit. Security, especially the more elusive cyber security, is particularly likely to be externalized in nonCIS firms because it is not deemed a profit center.

Furthermore, leaders and members of these enterprises are subtextually consistently discouraged from engaging in investments for longer term cyber resilience unless the effects of poor cyber security on the wider community are so immediate and disturbing that they rebound negatively and explicitly on the source firm itself in the near term. If not, then when mitigation of the risks involves uncompensated costs of any significance, such investments are to be instinctively viewed as unnecessary normatively, financially, and theoretically to market health of the nation and of that particular firm.

Given these motivation obstacles, the panel collectively suggested that motivating all three private actor communities would require framing the challenge differently by redefining elements of profit assessments to include cyber security investments explicitly. One way could be to recast and instantiate cyber security in terms of profit centers with a future positive revenue streams associated with better internal firm cyber resilience. Another would be to empirically, cognitively, and normatively integrate cyber security into profit consideration framed as an unavoidable revenue-depletion constraint that cannot be externalized to the wider community or viewed as irrelevant across firm actions. Government national security and other systemic databases and experiences can play a role in making cognitively and empirically clear how the wider systemic consequences of individually neglectful and non-cooperative actions in cyber security contribute cumulatively to reduced profit, devastated national markets, and accelerating declines in options for future domains over the near and long term across all enterprises. Public disclosure would be

an option to motivate companies to avoid bad PR. Over the short term, however, more efforts to drive tighter collaboration need be organized.

One specific recommendation was to encourage the inclusion in standard profit considerations of the need for life cycle costing (LCS) of losses over time due to cyber insecurities inside the firm, across its community and connected up or down stream partners, or endemic across its ecosystems. These would include latent, non-obvious knowledge investment, supply chain distortion, and market access losses among others elements which today constitute the 'greatest transfer of wealth in history" in the US alone.[3] Another approach is to include up and down stream liability on firms as key nodes and contributors to the cyber security or insecurity profile of the overall system.

Regulations are also motivators, imposed by governments to compensate for negative outcomes from aggregated firm behaviors across critical systems and markets. In complex socio-cyber-economic systems such as deeply digitized nations, the actions of one firm in its own self-interest that rebound on other firms and the rest of the national system negatively are a matter of public policy.[4] Firms are not necessarily opposed to regulations that clarify the market conditions, liabilities, and longer horizon domain expansion options, as long as the playing field remains on the same level for everyone. In some cases, regulations can serve as legal cover for what private firms see as necessary but cannot justify given the profit points made above. Regulations have the advantage of forcing near term actions depending on will and capacities of the political system enacting and enforcing them.

The CIS community including the telecoms industry in general are regulated sectors, even though they share the normative dislike for regulations in principle. For this group, to jumpstart more serious considerations of cyber security within key firms and across the wider system, cyber security regulations could be enhanced to include more effective
cyber security standards within the firm as well as across the firm's upstream and downstream networks. In particular, the issues for direct regulatory consensus include standards and possible cross-leveling of local adaptive costs to reduce overall system threats, and carefully designed

[3] Gen. Keith B. Alexander, Commander US Cyber Command describes cyberspace as ubiquitous and being militarized by hostile states already exploiting widely across the nation information stocks, including those essential for economic well-being, and calls it "the greatest transfer of wealth in history". (http://www.youtube.com/watch?v=jaaU5nGDh68)

[4] Observations by a senior Estonian ministry official when speaking on cyber security. This approach is also a subtext of the cyber strategy of several European nations.

evolution of legal liabilities to encourage near and long term internal innovations to improve hygiene, wider awareness, and transparency overall.

For the IT capital goods sector and the cyber victim enterprises, however, the use of regulations to catalyze better internal and collective cyber security will be viewed negatively, especially if cyber security costs are harder to externalize. They will be undoubtedly resisted normatively, professionally, and by lobbyists. To be effective, such regulations will need to promote technical and operational standards requiring an internalized, more holistic approach by individual firms to their own and their wider system's cyber security investments.

Metrics

The gap in modern systemic metrics for a cybered age directly hinders the ability of all three communities to contribute positively to national and international cyber security and the wellbeing of nations. On the most immediate level, such metrics simply lack data as sensors and logging are frequently insufficient to detect incidents, Also, the impact of many cyber incidents is hard to assess. Standard accounting and financial metrics fail to alert even the most cyber sensitive firms to the long term systemic losses from cumulating cyber insecurity across the system around them. Needed are easily absorbed alternative mechanisms to discern, for example, near and far term cyber losses in knowledge investments, in market dominance or access, in progress towards greater internal and systemic security, and in comparison with partners or competitors across markets, products, nations, or regions. Needed also are more systemic models of, for example, non-equilibrium socio-cyber-economic systems that include regulations and market processes of the emerging cybered age, as well as other models with different sector mixes and knowledge flows.

To be developed are ways to measure prevention/passive protection in relation to the firm's attractiveness and exposure as a target, especially those enterprises to be considered a part of the 'soft underbelly' of medium and small businesses employing the majority of citizens. Such metrics can reveal hidden dependencies, as well as support multi- stakeholder and collective national strategic assessments. Properly done, such metrics can also improve the foresight of all parties, increase transparency, and highlight the free riding actors avoiding costs through public relations or ornamental cyber hygiene assurances. .Combined with disclosure, metrics can help create peer pressure to act in ways supporting the whole system, and even the implementation progress of a nation's cyber strategy could be assessed more effectively than is remotely possible

today. A useful backdrop for any kind of metrics could be a definition of the "platinum class"[5] of technical, operational and strategic cyber security measures, so success can be measured as distance to an ideal state, relative to the appropriate risk model. Finally, appropriate metrics allow national protection efforts to be focused and adjusted at the right scale, foci, and alacrity needed to keep the whole socio-cyber-economic system adequately resilient
for national wellbeing.

Government collaborative efforts in research support, guidance, standards, as well as requirements for such models in, say, liability or regulatory negotiations are essential in nurturing development and acceptance of effective metrics. If the responsible actors in the organization do not know how to count what is essential to improve cyber security, then governments and collective sense-making programs need to step in. It has been noted throughout the literature on organization theory and policy studies that what one counts is what gets done in the organization. The gap in analyzing and instantiating due to missing metrics today means neither these communities nor the government have actionable indicators of sustainable socio-cyber-economic wellbeing for themselves or the system over the long term.

Structures

Private firms largely exist in competitive environments where sharing critically important knowledge is heavily discouraged as bad practice that endangers market share. Without structures of knowledge sharing considered neutral and non-threatening in routine business terms, firms do not share their data externally. As a result, data and insights critical to avoiding overall system surprise stays encased in individual firms' private databases. Missing for each firm is not only trust with other firms and with government agencies, but also the abilities to handle the feedback from large data systems across industries, regions, domains, and nations. Without this trust and sharing, lost to the wider community is knowledge to reveal emergent needs for more capacity in and across firms, to address advanced challenges, and even to deeply understand their own sector deep structures.

As the party ultimately responsible for the wellbeing of the entire nation, governments need to orchestrate and sustain neutral and systemic trusted data sharing structures for continuous, actionable knowledge sharing. For cyber issues, government action is required because voluntary

[5] S.Gaycken

associations necessarily have either a limited mandate or limited resources compared to the overarching complexity of the national system. Subscribers to industry specific cyber security groups do not have access to government intelligence and other data, and members are prone to withholding crucial data for highly individualized, proprietary, or unwitting reasons. As a group, they do not have the duty to prepare for the consequences of their actions in producing negative wider outcomes outside of their region or industry or domain.

The private sector communities, however, do have data to share if their trust in the security of their proprietary data is assured and if the structures for sharing also offer considerable monitoring and consequence recognition benefits currently unobtainable for these communities. In return, government sustained structures for continuous sharing of filtered, operationalized, timely, and activating cyber terrain data better accommodate the wider national need to identify emergent threats and their sources across the critical cybered systems. Institutional structures to accommodate both requirements will have to be jointly staffed with public and private actors at a minimum, and widely supported across government and all three communities, at a minimum.

One such structure that has existed for at least 25 years is the CERT-CC model of a private (university managed, private firm subscribed) computer emergency response team. While its original mission was limited largely to knowledge exchange among subscribers who provided data post hoc, its subsequent forms found at national levels with names such as CSIRT are more muscular and offer broader services in response mitigation and alerts. The next iterations of such models are likely to be both less voluntary and more regulating. However, this trend so far is less collaborative than could be the case when these structures are seen as mutually valuable.

One idea could be a national "cyber bridge6, in which the institutional structure operates as collective filter through which the government's and the private communities' knowledge critical to cyber security can be exchanged without revealing sources, methods, or proprietary data. It can also function as a shared 'cyber RAND' institution integrating the flows of data forward to inform all institutional parties of emergent trends and threats. Its capacities could include cyber ranges and a concentration of individuals with advanced cyber skills irrespective of institutional origins, and its products could help revenue streams in both public and private budgets. An advantage of a more

[6] Bill S.

collectively valued structure is the generation of more innovative responses, standards, and new baseline technologies. Another suggestion is to have regional data sharing that co-locates firms across industries with similar needs for collective cyber protection.

Beyond the reciprocal provision of data, however, is the possibility of sharing process knowledge and success experiences between government and private units with regard to crisis management. While most modern militaries expect to be surprised and prepare for crises as though they may occur at any time, the vast majority of private firms treat crises as failures that rarely, if ever, emerge if industry best practices are followed. They do not prepare as if they are routinely breached in cyber penetrations. Furthermore, for all the reasons discussed above, cyber crisis management that involves collective preparations with competitor firms is not encouraged in the way militaries proactively set up crisis orders and teams. Their crisis agility is focused on market surprises, not local or widespread, frequent cyber surprises. In contrast, militaries have a skill set that can be of help and can be shared under these knowledge exchange structures. Having the structures of shared, safe, directly usable knowledge exchange also encourages joint government-private development of situation awareness, of different perspectives and critical valuations of systems, and of mutually developed government-private crisis management.

Recommendations for engagement and norms development

If the motivations, metrics, and structures are collectively developed into shared daily practices across the three private sector communities and government elements to produce better cyber hygiene, resilience, and action as needed, then the norms so necessary to guide future actions and positive evolutionary trends will reinforce more civility as a standard motif internationally.