Norwegian Institute of International Affairs

Policy Brief
[20 / 2015]

Securing Cyberspace

Coordinating Public-Private Cooperation

Lilly Pijnenburg Muller

Summary

Modern society is increasingly dependent upon a well-functioning and secure cyberspace. However, the stability, growth and security of this infrastructure are not preordained: they must be facilitated. As over 90% of what constitutes cyberspace today is owned by the private sector they have a large role to play. Moreover, cyberspace knows no national boundaries, so the securing thereof must be conducted on an international scale with close cooperation between states and private sectors. This policy brief examines who should be involved in securing cyberspace, and how to do so. Cooperation programmes that follow a 'multistakeholder' model are widely seen as a panacea for securing cyberspace, and the model is employed in several current initiatives in the field of cybersecurity. However, this policy brief questions whether a multistakeholder model is the most appropriate approach. Public/private-sector collaboration within a state is essential, but for this to be effective it must approach the premises of the private sector. This policy brief recommends the creation of a network platform to coordinate efforts between the state and the private sector for responding to threats to a well-functioning cyberspace.[1]

1 'Cybersecurity' concerns threats to a well-functioning cyberspace. The threats may come from various types of malware, attacking the codes that make up cyberspace. When these codes are changed by actors other than those that 'own', or have created them, that is an 'attack'– and can spy on, steal, abuse and destroy digital information, even create physical and off-line effects. The various ways of altering a code are what separates viruses and attacks on cyberspace, but the core point is changes to code. These vulnerabilities arise not only from intentional agents but also from systemic threats that stem from the inherent unpredictability of computers and information systems which by themselves 'create unintended (potentially or actually) dangerous situations for themselves or for the physical and human environments in which they are embedded' (M.Dunn Cavelty, 2014, *Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities*. Zurich: Springer Science). These threats arise from software as well as hardware failures, and cannot be corrected by perfecting digital technology and programming: there exists an inherent ontological insecurity within computer systems. Cybersecurity is thus the response to these threats.

Cybersecurity and the multistakeholder model

Efforts to study and practice cybersecurity start from the premise that cyberspace is governed by an innovative, unusual (perhaps unique) 'multistakeholder' model. The term 'multistakeholder governance' came into use in the 'internet arena' around 2004.[2] Although there is no clear-cut definition of a multistakeholder initiative (MSI), most of the diverse initiatives referred to as MSIs are 'interactive processes in which business processes are more socially and/or environmentally sustainable'.[3] The executive coordinator for the Internet Governance Forum (IGF) secretariat, Markus Kummer, describes multistakeholder governance as a vehicle 'for policy dialogue where all stakeholders took part on an equal footing' via a process that is open, inclusive and transparent.[4] Further, 'while multistakeholder participants in the World Group on internet governance (WGIG) and IGF meant and means that all stakeholders participate on an equal footing, it is also clear that in most organizations, intergovernmental or not, there are some structures are in place to facilitate decision-making processes.'[5]

The features of cyberspace, especially the lack of an authoritative role for states in governing and securing it, have led scholars and practitioners to conclude that cyberspace provides an example (perhaps the only one) of multistakeholder

2 J. Savage and B. McConnell, B. (2015) Exploring MultiStakeholder Internet Governance, EastWest Institute. Available at http://www.ewi.info/idea/exploring-multi-stakeholder-internet-governance

3 W.v.Huijstee, (2012). 'MultiStakeholder Initiatives: A Strategic Guide for Civil Society Orga¬nizations', The Social Science Research Network, SSRN 2117933. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2117933

4 M. Kummer (2013). Multistakeholder Cooperation: Reflections on the emergence of a new phraseology in international cooperation, Internet Society. Retrieved from their web¬site: http://www.internetsociety.org/blog/2013/05/multistakeholder-cooperation-reflections-emergence-new-phraseology-international

5 Ibid.

governance.[6] Here ICANN – with responsibility for coordinating the of maintenance of several databases of unique identifiers related to the namespaces of the namespaces of the Internet,[7] and ensuring the network's stable and secure operation – is often cited as an example. This is because it seeks to bring all stakeholders together to participate in dialogue, decision-making and implementation of solutions to its problems or goals, on an equal footing. However, it is erroneous to speak of multistakeholder governance of cyberspace and of multistakeholder securing of cyberspace as a single concept. Various different bodies exert authority over related but distinct aspects of governing and securing the Internet's technical and structural architecture. Arguably, it is in the inaccuracy of seeing governance and the securing of cyberspace as a single entity that much of the confusion surrounding the possibilities of securing cyberspace through a multistakeholder approach originates.

Viewing multistakeholderism as a teleological goal for all aspects of cyberspace governance can create problems. A multistakeholder governance model is not appropriate in every functional area of governance in cyberspace.[8] Keeping cyberspace operational and secure involves coordination and policy-making. Identifying an appropriate approach to a responsible and efficacious cybersecurity requires determining what types of administration are optimal for promoting a balance of interoperability, innovation, functionality and operational stability. To do so we must understand how cyber security functions and who is included in this aspect of cyberspace. Drawing on DeNardis' separation of the securing of cyberspace into task and institutional actor can be helpful (see figure).[9]

Cybersecurity governance[10]

Task Cybersecurity Regulation/ Enforcement	**Primary institutional actor** National Statutes/Multilateral Agreements
Designing Encryption Standards	Standards-Setting Organizations
Securing Network Infrastructure	ISPs, Network Operators, Private End-user Networks
Correcting Software Security Vulnerabilities	Software Companies
Software Patch Management	Private End-users
Securing Routing, Addressing, DNS	Network Operators, IETF, Registries
Responding to Security Problems	CERTs/CSIRTs
Trust Intermediaries Authenticating	Web Site Certificate Authorities

6 For a practitioner's view, see the statements of the current ICANN CEO, Fadi Chehade, available at http://www.internetgovernance.org/2012/10/15/icanns-new-ceo-talks-about-balance-of-power/. For scholarly uses of the term multistakeholder governance, see Vint Cerf, Patrick Ryan and Max Senges, 'Internet Governance is Our Shared Responsibility ', *I/S: A Journal of Law and Policy* 10 (2014).

7 As Domain Name System, including policy development for internationalization of the DNS system, introduction of new generic top-level domains (TLDs), and the operation of root name servers.

8 M. Dunn Cavelty and M. Suter. (2009) 'Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection', *International Journal of Critical Infrastructure Protection*, (4): 179–87.

9 L. DeNardis and M.Raymond (2013), Thinking Clearly About Multistakeholder Internet Governance (14 November). Available at SSRN: http://ssrn.com/abstract=2354377

10 From DeNardis and Raymond (2013), 'Table 1. Disaggregated Internet Governance Taxonomy'

Only a small portion of what is included in securing cyberspace is the responsibility of the state, so to talk about a multistakeholder practice in securing cyberspace is misguided. With over 90% of cyberspace owned by the private sector, its say and impact are tremendous. To date two predominant characteristics of cybersecurity arrangements can be seen. First, states have been generally uninvolved, or involved only as participants, without superordinate decision-making authority.[11] Second, decision-making has typically been driven by technical and market considerations. One consequence of this is a lack of a clear division and understanding of who in government is to be involved in securing cyberspace –makes for a cumbersome coordination for cooperation with the private sector.

Scholarship on institutionalism in the international sphere has focused more on problems of coordination than of cooperation.[12] The interests of the private industry and the state are only partially convergent as regards to securing cyberspace, and synergy effects are not always easily achieved. For one thing, the transparency needed for a multistakeholder approach is neither viable nor realistic. From an economic perspective the private sector does not wish to openly share information on attacks it has experienced in cyberspace and detected weaknesses, as sharing this in accordance could both lower a company's credibility and stock value. Yet, it is not that the private sector is reluctant to cooperate with the public sector, but the coordination and capability within the government that is insufficient. This does not mean that some form of coordination between the public and private sector is neither possible nor desirable – quite the contrary. In Norway, for example, the level of cooperation between the public and private sector in governing and securing cyberspace is seen as advanced. Nevertheless, the coordination is often ad hoc and bilateral (between the government and individual private actors), with little overarching strategic planning or facilitation for coordination. There is great potential for improvement on the strategic and political levels, and a clear need for better horizontal, vertical and international coordination to secure cyberspace. Yet, so far, this has proven difficult to achieve.

Cooperation and coordination to secure cyberspace

Coordinating a cooperation mechanism between the public and private sphere domestically, and being able to communicate this on the international level, is difficult. Without a mechanism for coordinating internally how to cooperate in securing cyberspace, it is difficult to establish international cross-border cooperation. A mechanism for internal communication between the parties, with a way to communicate this outwards on the international level, is lacking in most countries. The potential terms for coordination need to be re-assessed to improve and elevate the current level of

11 This feature encapsulates part of what has been referred to as 'networked governance'. See M.L. Mueller, A. Schmidt and B. Kuerbis (2013), 'Internet Security and Networked Governance in International Relations', *International Studies Review,* 15 (1): 86–104.

12 On the implications of these styles of games, see L.L. Martin and B.A. Simmons (1998), 'Theories and Empirical Studies of International Institutions', *International Organization* 52 (4): 729–57.

cooperation. The interest and incentives to progress towards strategic planning and facilitation in securing cyberspace must come from the private and the public sector. Both sides have information and intelligence that the other side needs to attract them to the table. In contrast to other public–private cooperation, in the sphere of cyberspace the private sector has a greater impact, responsibility and say than with other commodities where the state cooperates with the private sector to secure its smooth functioning. Yet, although most of what constitutes cyberspace rests with the private sector, the responsibility for regulation and enforcement of cybersecurity still lies with the state. To lift cybersecurity to a strategic level the parties are dependent on each other, however the conditions for such cooperation today are few. A mechanism in the form of a network platform that brings together the public and private sector in a non-binding gathering could be one step towards strengthening cybersecurity through strategic coordination.

Incentive for cooperation through sharing mechanism: a network platform

A network platform that brings together high-level representatives from the public and the private sector can facilitate the possibilities for closer and improved public/private-sector cooperation in securing cyberspace. Based on the mutual benefit of sharing information the network platform can coordinate and create communication between the strategic and operational level through facilitating the exchange of information, knowledge, expertise and good practices. In this way it provides opportunities to all actors involved to influence the decision-making process, and brings networking opportunities. With regular and consistent communication and cooperation, information sharing becomes beneficial to both parties, improving both the national and international levels of cybersecurity. By bringing together high-level stakeholders from the relevant private sectors to communicate with the public sector, a unified voice can be established to represent the private sector to the public sector, and in turn to international forums. This can foster improved understanding of and between the parties involved.

A network platform moves towards creating a unified voice in securing cyberspace. At international forums, the state can, through its foreign ministry, gain information on cyber-attacks experienced by the private sector in other countries. This information is essential for establishing where new attacks may originate, and for identifying the perpetrators. Information can also be obtained on what security measures are being taken and what 'holes' other countries find that need to be patched. Since cyberspace operates beyond national boundaries, it is vital for all parties that this information is shared internationally. This is necessary for enabling the creation of a pre-emptive defence mechanisms and sensors to discover possible new attacks. And the converse: such information sharing must be reciprocated by the private-sector community in other countries, based on their experience in securing cyberspace. To facilitate this sharing, the public sector can through the network platform obtain similar information from the private sector in its respective countries, to be communicated back to international forums. By stimulating interaction among high-level stakeholders, including civilian and military government agencies, academia, businesses, civil society, internet providers, CERT and the technical community a network platform can achieve this synergy. This will help to move cybersecurity from ad hoc and bilateral agreements to the strategic and political level. A network platform that creates synergy between the parts may be based on an existing platform, or a new one can be created. What is crucial is that the network functions.

a) Create trust through sharing mechanisms
Through mutual regular communication and information sharing, incentives for trust are established. The state, having the most to gain from this mutual benefit, should take the first step by sharing information that the commercial actors need, thereby showing them that they too will gain from the cooperation.

b) Set clear goals
By establishing short- and long-term goals a network platform can play a part in establishing political priorities. It is important to set these goals with technical backing and an understanding of the issues central to cybersecurity for all stakeholders. Heeding the diverse voices collected through the network is crucial. By setting the goals in these premises they function to clarify areas of responsibilities and enhance cooperation between the public and private sector on the strategic and political levels.

c) Create framework for policy development
Cyberspace is developing rapidly which results in outdated policies. To avoid this frameworks should be created to serve as guidelines for the articulation of long-term policies and policy goals. Establishing such frameworks within the network platform enables the private sector to exert influence on policy. This works both as an incentive for the private sector to come to the table, and for them to abide by the policies created.

The functioning of the network platform

Private sector	Government
• Unify a voice to communicate to the state to present externally/internationally • Influence policy through information sharing	• Coordinate, stimulate and regulate the network by defining simple but formal rules of governance • Create framework conditions that allow the network to organize itself • Balance the role of business and CEOs in its policies • Publish and advertise successful results • Regulate and legislate

All actors in the network platform need to be involved on equal terms. The role of the state, as chief regulator and law enforcer, is to share information and coordinate and stimulate the network, whereas the private-sector actors function as main coordinators in creating goals and establishing a unified voice to present to the public sector and externally

in the international sphere. Through the network platform, members of the private sector can communicate and network amongst themselves, and share with the public sector their views on cybersecurity priorities, fostering the creation of a unified voice for international use. Information sharing allows for better transparency and cooperation, enabling greater coordination and administration of the many layers of distinct tasks concerning cyberspace. Sustainability of the network platform requires that the private sector continues to come to the table, to be heard and to influence policy. This can functions as an incentive for the private sector to use the platform as a decision-making arena, and to follow the policies agreed upon. The network platform provides a mechanism to include the private sector in international discussions on securing cyberspace. Unlike the 'quick fix' of the multistakeholder approach to cybersecurity, a network platform can create a unified voice outwards: a first step towards coordinated cooperation in securing cyberspace where all stakeholders take part.

Conclusions

The idea of a multistakeholder approach to cybersecurity is not easily implemented in practice. To do so– according to the definition of a multistakeholder approach – would mean that all stakeholders take part on an equal footing in a process that is open, inclusive and transparent. However, with so much of cyberspace in the hands of the private sector, combined with the worries of security issues and economic risk that would follow such transparency around cybersecurity, this type of multistakeholder approach is neither viable nor realistic. For collaboration between the public and the private sector to be continuous, lasting and functional, it must approach the premises of the private sector. The public sector must demonstrate to the private sector that it will gain from such cooperation – by creating incentives and trust through information sharing. Both the public and private sector must be involved, to ensure a coherent and cohesive cyber security. A network platform for high-level representatives from the public and private sphere could promote communication between the public and private sectors, allowing cooperation in securing cyberspace to be elevated to strategic and operational levels. This can reduce coordination problems regarding cooperation and create synergy. Building on existing cooperation, the network platform can enhance coordination and lift it to a strategic level. Such a model is no quick-fix, silver bullet – but it is realistic and has potentials beyond the multistakeholder model.

Funded by the Norwegian Ministry of Foreign Affairs.

Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

About the Author
Lilly Pijnenburg Muller is a Junior Research Fellow in the security and defence group at the Norwegian Institute of International Affairs. Her research focus is on cybersecurity and cyber capacity building, global governance and public private relationships. She holds a MA in politics from the University of Glasgow.
lilly.muller@nupi.no

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PO Box 8159 Dep. NO-0033 Oslo, Norway
www.nupi.no | info@nupi.no