4. Cooperative Measures for International Cybersecurity

Paul Meyer*

Cooperative security today appears to be a tenet honoured more in the breach than the observance. This contrast is particularly striking in the new security environment of cyberspace. The special character of this space, a human creation that has grown exponentially in magnitude and utility for global society in the time span of a generation, might with sufficient political will have spared it from the forces of interstate conflict, but this has not been the case. The militarization of cyberspace is proceeding apace and those constituencies that might have prevented this trend and maintained a sanctuary status for this unique environment were too unaware or too unorganized to mount an effective defence.

According to a 2013 study by the United Nations Institute for Disarmament Research, 47 states with national cybersecurity policies assigned some role to their armed forces even though only six states had at that time published military cybersecurity strategies.[1] The United States has, as it so often is in international security matters, been a pace setter with respect to the military use of cyberspace. It created a distinct Cyber Command in 2009 with an initial budget allocation in fiscal year (FY) 2010 of US$ 114 million. This funding level was quadrupled to US $466 million for FY 2016. A parallel augmentation of personnel levels has occurred of the command's Cyber Mission Force. The number of cyber teams is currently 123, comprising 4990 people en route to a goal of over 6100 by FY 2018.[2]

Admiral Michael Rogers, the head of both US Cyber Command and the National Security Agency, has been explicit in Congressional testimony about the states that pose a cybersecurity threat to the United States—Russia, China, Iran and North Korea, in descending order of capability—and the need to generate a 'complete spectrum of capabilities', both offensive and defensive, to counter such threats. He has also advocated for the development of a 'cyber deterrence policy' for the USA, the absence of which would amount to a 'losing strategy' for the nation.[3]

While other states do not normally match the USA's high standards of transparency in military matters, it would appear that many armed services are establishing cybersecurity entities and developing their cybersecurity capabilities. This is particularly significant when 'offensive capabilities' are included in the mix, or the capability to engage in cyber operations with an extra-territorial disruptive, damaging or destructive effect. Admiral Rogers' affirmation that the USA will seek the same military supremacy in the cyber realm as it does in other operational domains will no doubt spur potential adversaries to try to counter this and in so doing contribute to a nascent cyber arms race.

Arguably, the first weaponization of cyberspace occurred some time in 2009–10 with the revelation that the so-called Stuxnet computer virus had been detected. This virus was a sophisticated cyber payload that targeted the computer-based control systems for the centrifuges used to enrich uranium at a nuclear facility in Iran. Stuxnet essentially caused the centrifuges to self-destruct, resulting in significant setbacks for

[1] United Nations Institute for Disarmament Research, *The Cyber Index: International Security Trends and Realities* (UNIDIR: Geneva, 2013), <www.unidir.org>.

[2] Statement by Admiral Michael S. Rogers, Commander, United States Cyber Command, before the Senate Armed Services Committee, 5 Apr. 2016, <www.armed-services.senate.gov>, p. 6.

[3] Statement by Admiral Michael S. Rogers (note 2), during oral testimony.

*The views expressed in this article are the author's and do not necessarily represent SIPRI, CISD/SOAS or the organizations with which the author is affiliated.

the Iranian nuclear programme. While there was never any formal acknowledgment of responsibility for the attack, media leaks have attributed it to the USA probably in partnership with Israel. Stuxnet represented the first use of what can be considered a cyber weapon: a payload that actually caused physical damage and destruction, or 'kinetic effects' in military parlance.

This move on the part of a leading state from cyber defence to cyber offence had major implications. In the words of General (ret) Michael Hayden, a former director of the National Security Agency and the Central Intelligence Agency: 'Somebody has used an entirely new class of weapon to effect destruction. Somebody's army has crossed the Rubicon, and we've got a legion on the other side of the river now, and it's not going back'.[4] Hayden's view is clearly that cyber weapons and presumably cyberwar are irreversible realities the world must accept. His interviewer however observes that Caesar's action in crossing the Rubicon was in violation of Rome's law, and implies that legal restraints will be needed to avoid the devastation that unbridled cyberwar could bring in its wake.

A further challenge to maintaining a peaceful cyberspace is the linkage to outer space, an environment that has similar importance for society's well-being and is also vulnerable to deliberate acts of destruction. All space operations have a cyber dimension as the communications between the 1300 active satellites in orbit and their ground stations are conveyed via cyber systems. Such signals are vulnerable to jamming to deny functionality, or 'spoofing', which can allow attackers to take control of a satellite. There have been several reports of cyber attacks against operational satellites including alleged Chinese cyberattacks against US remote sensing and meteorological satellites, although the details are often cloaked in secrecy.[5]

These steps in the 'militarization' of cyberspace have not gone completely unchallenged, although it is evident that action on the military side has far outstripped that in the diplomatic arena. The potential for preventive diplomacy in the context of international cybersecurity has not been sufficiently acknowledged or acted on. As a *New York Times* editorial notes: 'Cyberwarfare has already done considerable damage and can lead to devastating consequences. The best way forward is to accelerate international efforts to negotiate limits on the cyberarms race, akin to the arms-control treaties of the Cold War'.[6]

Such a clear prescription has not been taken up to date, however, by the leading cyber powers that could energize efforts to establish 'rules of the road' for international cybersecurity. Although the call to develop 'norms of responsible state behavior in cyberspace' has been echoed many times since the Obama Administration first put this goal forward in its May 2011 *International Strategy for Cyberspace*,[7] diplomatic progress to realize such norms has been sluggish. This may in part be due to the fact that while the USA was the first to articulate the need to forge a global consensus around such norms, it was Russia and China that were the first to formulate a set of norms and put it before the UN for consideration. The Sino-Russian draft 'International Code of Conduct for Information Security' of September 2011 had an ambitious provision for states 'not to use ICTs [information and communication technologies] including networks to carry out hostile activities or acts of aggression, pose threats

[4] Cited in Bamford, J., 'What @Snowden told me about the NSA's cyberweapons', *Foreign Policy*, 29 Sep. 2015.

[5] Robinson, J., 'Governance challenges at the intersection of space and cyber security', *Space Review*, 15 Feb. 2016.

[6] *New York Times*, 'Arms Control for a Cyberage', 26 Feb. 2015.

[7] White House, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (May 2011), <www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

to international peace and security or proliferate information weapons or related technologies'.[8]

This formulation proved problematic from a number of perspectives, not least the inherent ambiguity of terms such as 'hostile activities' or 'proliferate information weapons'. The Sino-Russian sponsors held sustained consultations at the UN on their draft set of norms, but the focus was more on domestic controls than arms control and it was based on a concept of 'information security' that was not universally shared. In January 2015 China and Russia circulated a revised version of their proposal. It dropped the arms control provision in favour of a more modest exhortation that states should refrain from activities 'which run counter to the task of maintaining international peace and security'.[9]

While the Code of Conduct proposal remains on the table, the principal focus of attention at the UN in recent years has been on a process involving a series of reports from the UN Group of Governmental Experts (GGE). This mechanism has involved groups of 15 to 25 government-nominated experts examining 'Developments in the field of Information and Communications Technology (ICT) in the context of international security'. These groups produced consensus reports in 2010, 2013 and 2015, the focus of which was increasingly on the development of norms for responsible state behaviour in cyberspace and the confidence-building measures that could accompany them.

The 2013 report had already flagged the risk to international peace and security represented by the lack of agreed norms for state behaviour in cyberspace. The 2015 report set out a bleaker depiction of the cybersecurity environment, which highlighted 'a dramatic increase in incidents involving the malicious use of ICTs by state and non-state actors'. It also recognized that 'a number of states are developing ICT capabilities for military purposes' and that 'The use of ICTs in future conflicts between States is becoming more likely'.

Against this darker threat assessment, the report emphasized the development of 'voluntary, non-binding norms for responsible State behaviour…that can reduce risks to international peace, security and stability'. Among the specific recommendations were that:

1. 'States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
2. States must not use proxies to commit internationally wrongful acts using ICTs;
3. States should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
4. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities.
5. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams of another State. A State should not use authorized emergency response teams to engage in malicious international activity.'[10]

[8] United Nations, General Assembly, International Code of Conduct for Information Security, A/66/359, 14 Sep. 2011.

[9] United Nations, General Assembly, International Code of Conduct for Information Security, A/69/723, 13 Jan. 2015.

[10] UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015.

Although these measures are all voluntary and there is no multilateral capacity to monitor their implementation, it is evident that they reflect an effort to apply existing principles of international humanitarian law to state conduct in cyberspace. In particular, to preclude attacks against critical infrastructure vital for civilians and attacks by or against emergency response teams to computer emergencies or cyber incidents, there are moves to give such teams a 'protective status' akin to that accorded the Red Cross and other humanitarian agencies under the Geneva conventions.

The concept of state responsibility for actions committed on their territory was reaffirmed in the GGE report, which also called for cooperation in responding 'to requests from other states in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory'. Given the challenge of attribution in cyberspace and the absence of any international system of monitoring, it could prove difficult to assess compliance with these norms in the months to come. Some recommendations of the 2015 GGE verge on the wishful thinking, such as the call to report on and share information regarding ICT vulnerabilities— the very thing that states exploit to carry out cyberattacks. Overall, however, the 2015 GGE made progress compared to its predecessors in specifying the nature of the confidence-building measures and norms for responsible state behaviour it wanted to see implemented.

While some at the UN admit to a degree of GGE fatigue, Russia and associated states were able to rally support for yet another GGE to get under way in 2016, with a reporting deadline of 2017. Although it may prove difficult for this GGE to add value to the findings of its predecessors, in the absence of any other authorized multilateral negotiating process on norms for responsible state behaviour, the UN GGEs with their broadly representative nature and consensus-based decision making will provide the international community with a credible vehicle for norm development.

This assessment of cybersecurity diplomacy has focused on the UN, and a technology as universal as the Internet certainly demands norms of global application, but there has also been some movement on cybersecurity cooperation at the regional level. The OSCE agreed an initial set of cyber confidence-building measures in December 2013. These voluntary measures dealt largely with information exchange and their degree of implementation is difficult to judge, although the OSCE did provide some institutional follow-up by establishing an Informal Working Group that will meet not less than three times per year to review the initial set of measures and consider the development of a second set. This envisaged second set has recently seen the light of day and reflects a general recognition of the need to make progress on cybersecurity norms despite the deterioration in East–West relations in the wake of Russia's intervention in Ukraine.

Other regional organizations, such as ASEAN, the ASEAN Regional Forum, the Organization of American States, the African Union and Asia Pacific Economic Cooperation, have also begun to consider interstate confidence-building measures on cyber activity, but they seem to be progressing more slowly and focusing more on cooperation in relation to countering cybercrime rather than governing interstate cybersecurity operations. The limited progress on establishing bilateral (US–Russian and US–Chinese) confidence-building measures or cybersecurity dialogues appears to be a function of their vulnerability to the vagaries of bilateral relationships. The US–Russian cybersecurity dialogue, for example, despite having generated an initial set of confidence-building measures, remains frozen.

China broke off participation in an embryonic bilateral cyber working group in the wake of the US Justice Department issuing indictments against five serving officers of the People's Liberation Army in May 2014 for allegedly undertaking cyber espionage

activities against US corporate entities. Chinese–US cybersecurity relations took a turn for the better after President Xi's state visit to Washington, DC, in September 2015 and the understandings reached then regarding limits to cyber-enabled economic espionage. A High-level Joint Dialogue on Cybercrime was established in the wake of the Xi–Obama meeting and met subsequently in December 2015 and June 2016. A related Senior Experts Group on international norms in cyberspace has also met. It is not clear how far these mechanisms have been able to address the military dimensions of cybersecurity or whether it will be possible to devise cooperative security measures to govern the cyber operations of the two powers. The fact that communication channels have been established is a positive sign and a necessary condition for embarking on more significant cooperation. The continued absence of a similar dialogue in the Russian–US context is disconcerting and may make it difficult to achieve broader cooperative security arrangements in cyberspace.

Conclusions

International cybersecurity policy is in an embryonic and hence fragile state. The vitally important realm of cyberspace has hitherto been essentially free of destructive state action. Stuxnet demonstrated that the weaponization of this unique environment is a real threat and that diplomatic efforts on cooperative security approaches have not kept pace with military capacity building. The recommendations on confidence-building measures from the UN GGEs require serious take-up by concerned states if they are to have any material impact on state conduct in cyberspace. Revitalized cybersecurity diplomacy is called for if cyberspace is ever to be preserved for peaceful purposes.

That revitalization will first and foremost require leadership on the part of one or more cyber powers. The USA, as noted above, arguably has the most at stake in providing for a cyberspace in which the threat of hostile action has been eliminated or mitigated. It will now be for a post-Obama administration to pursue with more vigour the forward-looking directions set out in the 2011 *International Strategy for Cyberspace* with its call for a global consensus to be forged on norms for responsible state action. This consensus might have to be built up incrementally through a set of arrangements worked out bilaterally between the leading cyber powers rather than through a comprehensive process at the universal level. Recent progress on the bilateral cybersecurity track between the USA and China augurs well in this regard.

Devoting the necessary political and diplomatic energy to making progress in regional security organizations is still highly desirable if common standards of state conduct in cyberspace are ever to be codified. An unheralded example of steady progress in hammering out such standards was the March 2016 decision by the OSCE to add a further five confidence-building measures to the initial set agreed on in 2013.[11] The new measures include facilitating exchanges on securing critical cyber-enabled infrastructure. This in turn could yield agreement on cooperative measures such as prohibitions on disrupting cyber communication links with satellites or other vulnerable critical infrastructure assets. The existence of an ongoing OSCE discussion on cyber confidence-building measures has also allowed for engagement with Russia and the USA at a time when bilateral channels of cooperation have largely been shut down.

A combination of self-restraint and self-interest on the part of the cyber powers may keep cyberspace from being transformed into simply another 'domain' of military conflict. The international community, including its billions of 'netizens', would no

[11] Organization for Security and Co-operation in Europe (OSCE), Confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies, Decision no. 1202, PC.DEC/1202, 10 Mar. 2016.

doubt prefer a more solid and transparent basis for sustaining a peaceful cyberspace. It will require continued advocacy and activism to ensure that states really behave in cyberspace in the responsible manner they publicly espouse.