

# From Chaos to Collective Defense

- ➔ **James Bret Michael**, *Naval Postgraduate School*
- ➔ **Eneken Tikk**, *Cooperative Cyber Defence Centre of Excellence*
- ➔ **Peter Wahlgren**, *Stockholm University*
- ➔ **Thomas C. Wingfield**, *George C. Marshall European Center for Security Studies*



**Deterrence, civil defense, collective defense, and arms control were key national security doctrines in the 20th century, and they are being reevaluated now for application to cyberspace.**

**T**he 1 July 2010 issue of *The Economist* covered several of the global information grid's systemic weaknesses that were uncommon knowledge to the public. Among other points, the article stated that "More than nine-tenths of internet traffic travels through undersea fibre-optic cables, and these are dangerously bunched up in a few choke-points," and "Internet traffic is directed by just 13 clusters of potentially vulnerable domain-name servers" ("War in the Fifth Domain: Are Mouse and Keyboard New Weapons of Conflict?" 3 July 2010, pp. 25-26, 28). A companion piece argues for arms control to reduce the danger to these weak links ("Cyberwar: It Is Time for Countries to Start Talking about Arms Control on the Internet," *The Economist*, 3 July 2010, pp. 11-12). This reflects a larger movement in legal and policy circles, most notably among the Russians, to reconsider arms control methodologies pioneered during the Cold War and determine if they can be applied to "the fifth domain."

There are essentially two types of arms control: structural, which limits things such as missiles and

tanks, and operational, which proscribes certain activities such as manufacturing chemical weapons or weaponizing biological agents. Structural arms control in cyberspace is difficult if not impossible, given the nature of cyber weapons, the importance to nation-states of maintaining their access to cyberspace for all aspects of warfighting, and nonstate actors' participation in cyber-based warfare and crimes. Operational arms control offers more promise—particularly when combined with complementary approaches such as deterrence through preparedness and collective defense.

Structural arms control is impractical and difficult to enforce in cyberspace. Instead, we suggest that progress be made to curb aggression and national security threats in the cyber domain by elaborating a strategy combining proactive technical and legal means with operational arms control and deterrence.

## PROTECTING ACCESS TO CYBERSPACE

Cyberspace access has been elevated to a national security concern in most nations because of

the integral role information and communication technology (ICT) play in most aspects of private and public affairs. Actions against this critical infrastructure can be criminal, requiring a law enforcement response; involve espionage, which demands action by a country's intelligence community; or even come in the form of an armed attack that permits military self-defense by a nation's armed forces.

This new arena has understandably produced many historical analogies, none of which are sufficient to address the novel circumstances of cyberspace. The nuclear analogy presents the most serious case. At the 1955 Geneva Summit, US President Dwight Eisenhower stated that the "nuclear genie" is forever out of the bottle. It became apparent to his successors that "nuclear disarmament is no longer a technical possibility" (Stanford Arms Control Group, *International Arms Control: Issues and Agreements*, J.H. Barton and L.D. Weiler, eds., Stanford University Press, 1976, p. 103). Although the cyber equivalent has also escaped the bottle, it isn't possible to put the genie back in through disarmament,

nonproliferation treaties, or other forms of structural arms control.

Unlike weapons of mass destruction, cyber weapons are an integral part of the commander's arsenal in conducting force-on-force and asymmetric warfare and will be used in concert with kinetic weapons to soften up the adversary's defenses. According to the 2010 US Department of Defense's *Quadrennial Defense Review Report* (Washington, D.C., February 2010, pp. 91-92):

A failure by the Department to secure its systems in cyberspace would pose a fundamental risk to our ability to accomplish defense missions today and in the future. Attacks in cyberspace could target command and control systems and the cyberspace infrastructure supporting weapons system platforms.

Most of the world's information infrastructure is owned privately and operated for civil use. Thus, the methods used for cyber attacks on national security are essentially the same as those used by cyber criminals, with the purpose and use of particular assets being the key distinguishing factors. In particular, developing a structural arms control treaty dealing with cyber weapons would be legally and technologically challenging. International law typically lags years behind the introduction of new weapons. In cyberspace, new weapons—including new types of weapons—appear all the time.

A further complication is that ICT can be dual-purpose, making it challenging to definitively determine that an ICT artifact, such as a cloud computing service, is a cyber weapon.

In addition, some ICT artifacts have been designed to be lawful, as was shown for so-called "software decoys" that serve as an airlock between technology and the law (J.B. Michael and T.C. Wingfield, "Lawful Cyber Decoy Policy," D. Gritzalis et al., eds., *Security and Privacy in the*

*Age of Uncertainty*, Kluwer Academic Publishers, 2003, pp. 483-488). Decoys can be programmed with a spectrum of options for taking action and providing anticipatory exception handling. We can develop policy that places boundaries on the extent and type of deception employed but provide latitude for cyber operators to inject creativity into deceptions to increase the likelihood they will be effective; the boundaries delineate thresholds that, if breached, would result in misuse or unlawful use of decoys.

Virtual inspections for cyber weapons might be possible, but it's difficult to determine if we've been deceived by an artificial construct mimicking the capability to be inspected. As was found in trying to apply structural arms control for chemical weapons, developing treaties for cyber weapons is complicated because the weapon components are broadly used in the ICT industry: how they're assembled into systems determines their use. Moreover, defining specific cyber sites for inspection is difficult: the horizontal diffusion of cyber technology and potential weapons capability makes inspection several orders of magnitude more complex than for kinetic weapons.

We also need to ask, "Which 'weapons' should be controlled?" The useful life of cyber weapons is short relative to that of kinetic weapons, due in part to technology churn. Any treaty specific enough to be enforceable against a particular threat would be obsolete long before deployment. Furthermore, there's no need to stockpile cyber weapons because they are readily replicated and distributed. It's also hard to determine whether all copies of a weapon have been destroyed. Obfuscation techniques, such as polymorphism, encryption, steganography, and malware embedded into firmware or hardware only add to the complexity of detecting the presence of cyber weapons. Automated tools could assemble weapons

just-in-time from artifacts that appear otherwise benign.

Furthermore, in contrast to the case of nuclear and other types of kinetic weapons, there are no commonly agreed-upon metrics for reporting the yields of a cyber weapon. Metrics must account for more than just first-order effects. Cyber test ranges aside, software behaves according to the environment in which it executes, that being the Internet. Testing cyber weapons to determine their yields would be difficult for many reasons, such as legal and policy constraints on performing the assessments outside of isolated (from the Internet) environments. Use of cyber weapons of unknown pedigree or yield might not be a concern of those actors who ignore the laws of information conflict, but it is of great concern to lawful combatants.

The absence of market incentives will require a well-thought-out, top-down, government-driven initiative to more quickly and efficiently fill in those gaps that markets cannot. Tailoring cooperative initiatives directly around these areas of market failure, or at least lack of market interest, would ensure that governments and markets each do what's best in the cyber realm.

To the extent that Russia is not reassured by closer cyber cooperation among NATO members, collective security must reach beyond NATO's borders to avoid the appearance or reality of a zero-sum confrontation. There may be room for a much larger conception of collective security that includes non-NATO countries such as India, Japan, and South Korea.

No policy works if it's orthogonal to persistent incentive structures. To build a truly effective international cyber security structure, we need a depth of initiative beyond a stereotypical operations center that can detect and avert a hypothetical cyber attack. Collective security in the real world would involve a longer time frame and such components as regulatory

adjustments, product inspections, and a first-class training program to instantiate best practices in the operational community. However, efforts such as government-based product inspections are challenging to implement and make effective (B. Michael, "Are Governments up to the Task?" *IEEE Security & Privacy*, vol. 6, no. 6, 2008, pp. 4-5).

## DETERRENCE IN CYBERSPACE

At the force-on-force level, superpowers are equals because they can deter their counterparts from all-out attacks. Cyberspace has punitive deterrence through threat retaliation. An attacked nation could respond via a combination of diplomatic actions and military might beyond a purely cyber counterattack, possibly involving kinetic weapons, although probably not more destructive weapons. Short of the Cold War's mutual assured destruction (MAD), however, punitive deterrence will likely be ineffective against nonstate actors and rogue nations intent on spreading terror at any cost. Despite undeniable areas of conflict and competition, superpowers thus share several common interests in cyberspace: a quick response to cyber attacks that minimizes risk of partial or full loss of access to cyberspace; concern about disorder introduced by rogue nations and nonstate actors such as terrorist organizations; cooperation and transparency in many areas where the interests of even antagonist powers are common; and clarity on the international legal standards that apply.

Countries defending themselves in cyberspace tend to operate in a legal gray area: the level of actual or potential damage clearly demands national-level attention but might not rise to the level of an armed attack under international law.

Aggressors benefit from this legal uncertainty. Shrinking the gray area gives cyber operators and national decision-makers greater confidence

in a clearer set of defensive options.

Today, the three criteria for active defense in peacetime are necessity (exhausting all peaceful alternatives with a reasonable prospect of success), proportionality (doing no more damage than must be done to neutralize the immediate threat and prevent it from re-engaging), and imminency (ensuring the enemy is "irrevocably committed" to the attack before launching a preemptive defense strike—either at the incoming weapon, or a support network necessary for its success).

Providing mutual assistance in "peacetime" works within the framework of existing alliances and regional organizations, but few cyber powers (nations with the wherewithal to conduct large-scale cyber campaigns) find themselves thus aligned. One problem is the cyber force-on-force threats posed by each of the cyber powers. In day-to-day operations, this is largely a matter of intelligence operations and espionage, which seek to obtain information without leaving any trace or alteration in the examined system.

In high-end espionage, covert operations straddle the legal world between intelligence collection and military operations. Covert operations often aim at leaving artifacts in a system, permitting anything from easy return access to remote-controlled sabotage. This type of operation and the potential damage it causes to a nation's defenses make it vital that international lawyers and computer technologists collaborate to identify lawful thresholds for operational action.

Space and time compression in cyberspace can cause many simultaneous effects at numerous locations, just as many actors (such as "patriotic hackers") can combine their capabilities to form mass effects at a chosen place and time. To address these factors, cyber powers must tailor their "presence" in cyberspace to be "vis-

ible," such that it serves as a deterrent against malefactors.

Preparedness and collective defense are viable forms of denial deterrence in cyberspace for all types of actors. Just as a defender can use strong encryption to deny an adversary the ability to gather information to plan an effective attack, being prepared across legal, policy, and technical dimensions will act as a deterrent to would-be aggressors (J.B. Michael et al., "Integrating Legal and Policy Factors in Cyberpreparedness," *Computer*, vol. 43, no. 4, 2010, pp. 90-92).

## COLLECTIVE DEFENSE

Collective defense poses a challenge for cyber powers, but even here their interests are unthreatened when smaller powers combine to provide better situational awareness against mutual threats—including some that would otherwise use small nations' systems to hide between attacks on the great powers. The analogy of "draining the cyber swamp" to make the ungoverned spaces less safe for cyber terrorists offers a powerful incentive.

John Arquilla argues that through illuminating and infiltrating terrorist networks in cyberspace, "our enemies ... would likely flee cyberspace, as this medium could no longer be trusted. This would unravel the 'virtual caliphate [of al Qaeda]'; impede support functions and, more generally, slow down an already pretty slow operational tempo in the field" (J. Arquilla, *Aspects of Netwar & the Conflict with al Qaeda*, Naval Postgraduate School, 2009).

Collective self-defense is a term of art in international law. The mechanism of collective defense derives from Article 51 of the United Nations Charter, whereby an "armed attack" activates the "inherent right of self-defense," either individually or collectively. This same standard is applied by regional organizations, most notably NATO. Under the Wash-

ington Treaty, NATO countries are bound to defend each other in an attack. The most important prerequisite for collective self-defense is the threshold of an armed attack: something we haven't yet witnessed with any of the known international cyber incidents.

As serious as the 2007 cyber attacks against Estonia were, few argued they were the legal equivalent of "tanks across the border." Tanks literally crossed Georgia's border in 2008, so the question of whether the incursion's cyber components would have risen to the level of armed attack never occurred. Even an attack that rose to the level of widespread destruction would come from a primarily political decision to engage in cyber war. This makes it critical for nations to consider their collective interests and build "cyber coalitions" in which analysts view threats and defense in a similar setting. Gradually, understanding would create deterrence in itself as the legal framework applied to a cyber-armed attack would give the target nation many tools and remedies compared to the gray area below the law of armed conflict.

### OPERATIONAL ARMS CONTROL IN CYBERSPACE

Operational arms control plays a role in cyberspace. According to Pál Dunay, the four discernable types of operational arms control are measures to: facilitate communication in a crisis or, in general, reduce secrecy and increase transparency in military matters, make force postures less offensive, and indirectly decrease the reliability of armed forces and their weapons (P. Dunay, "Arms Control in the Post-Cold War World," P. Dunay et al., *Open Skies: A Cooperative Approach to Military Transparency and Confidence Building*, United Nations Institute for Disarmament Research, 2004, pp. 5-16).

Let's consider the case of implementing transparency measures by

improving the exchange of information among nations about best practices for minimizing interactive complexity and coupling in cyber weapon systems. These systems are known contributors to what Charles Perrow terms "normal accidents," mishaps from unanticipated interaction of multiple forces in a complex system (*Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, 1999). Complex interactions in this context are "those of unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible." We can envision the possibility of an actual mishap such as an inadvertent launch of cyber weapons against a nonexistent threat because of false information provided by cyber-based sensors, which in turn results in an armed conflict. Perrow affirms this point:

The defense system is one that grows in complexity. We are not merely adding safety devices to buffer a failure ... [because] the "failures" we must guard against are those that an enemy (supremely clever and resourceful, it is assumed) is actively promoting. Each side mindlessly makes it less possible for the other to rest assured that it does not seek its total destruction.

The expansion of cyberspace renders traditional legal and policy approaches to solve problems ineffective. Similarly, the speed and opacity of cyber operations, as well as the rapid development of subjects that might be used as cyber weapons, makes strategies for relying on structural arms control inappropriate. The nonstate nature of many cyber actors is another factor hampering such a course of action.

**A**dmittedly, the legal, policy, and technological demands raised here are daunting, but the real-world benefits would eventually outstrip past doctrines.

Handling threats of this complexity requires multifaceted skills based on technical and legal insights. A robust cyberspace is not only an ICT phenomenon but a system of technical components incorporating organizational and legal solutions, defined and implemented proactively. Relying on traditional military, legal, and technical remedies is too simplistic. Deterrence and operational arms control alone will not suffice. **□**

*James Bret Michael is a professor of computer science and electrical engineering at the Naval Postgraduate School. Contact him at [bmichael@nps.edu](mailto:bmichael@nps.edu).*

*Eneken Tikk is a legal advisor at the Cooperative Cyber Defence Centre of Excellence located in Tallinn, Estonia. Contact her at [eneken.tikk@ccdcoe.org](mailto:eneken.tikk@ccdcoe.org).*

*Peter Wahlgren is a professor of law and information technology at Stockholm University. Contact him at [peter.wahlgren@juridicum.su.se](mailto:peter.wahlgren@juridicum.su.se).*

*Thomas C. Wingfield is a professor of international law at the George C. Marshall European Center for Security Studies. Contact him at [thomas.c.wingfield@marshallcenter.org](mailto:thomas.c.wingfield@marshallcenter.org).*

**Editor: Jeffrey Voas, National Institute of Standards and Technology;**  
[j.voas@ieee.org](mailto:j.voas@ieee.org)

### Disclaimer

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements of their respective governments.

**cn** Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.