politique étrangère

The Incomplete Governance of the Internet

Ebola: What Should Have Been Done

Winter 2014–2015

ifri

The Virtual Weapon: Dilemmas and Future Scenarios

By **Lucas Kello**

Lucas Kello is a Senior Lecturer in International Relations at Oxford University and an Associate of the Harvard Kennedy School's Belfer Center for Science and International Affairs.

The cyber revolution challenges conventional mechanisms of deterrence and conflict management. It is difficult to attribute responsibility for and even detect cyberoperations. The growing ability of nonstate actors to conduct offensive action further complicates the design of measures to repulse it. A large-scale cyberattack could instigate an intensifying spiral of escalation involving conventional strikes.

politique étrangère

There is hardly a more pressing topic in contemporary security affairs than the cyber danger; yet none so perplexing. The virtual weapon is a recent addition to the arsenal of states.[1] Security planners have yet to decipher its meaning for strategy. Only a limited record of events exists to orient this laborious learning process. The new capability, moreover, is scientifically complex and highly volatile. Even computer specialists do not fully grasp its behavioural properties or the consequences of its use. One thing however is becoming clearer: the cyber phenomenon challenges inherited security mechanisms.[2] Two core questions of strategic theory stand out in relation to this problem: How to deter a major cyberattack? How to control a cyber conflict following a failure to deter?

Prevailing strategic doctrine gives no satisfactory answer to these conundrums; it prescribes remedies to solve the one that exacerbate the other. Computer network operations are very difficult to thwart.[3] Consequently,

1. Cyber arsenals however are growing steadily. Over one hundred states possess or are assembling virtual stockpiles. See W. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* (September/October 2010.
2. For a discussion of how the cyber phenomenon challenges strategic theory, see J.S. Nye Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, vol. 5, no. 4, Winter 2011, p. 18-38; and L. Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, vol. 38, no. 2, Fall 2013, p. 7-40.
3. Possible targets for such attack include the London Stock Exchange or RTE, France's electricity-grid operator.

the temptation of deterrence policy is to express a readiness to resist attack with the maximum of credible force—the so-called "equivalence principle," which stipulates that a major cyberattack may elicit a conventional military reprisal, without however clarifying thresholds for such a response. The promise of severe penalties produces pressures for an accelerating crisis should an exchange of blows occur. Thus measures to bolster deterrence elevate the risks of unwanted escalation if deterrence fails.

This article examines the implications of cyberweapons for logics of deterrence and conflict escalation—and their interrelation—in three steps. First, it discusses the nature of the cyber phenomenon in general theoretical terms, drawing on concepts in the study of international relations to elucidate its effects on security relationships. Second, it reviews the challenges of deterring a major cyberattack in the absence of viable options to repulse it. Third, the study analyses the risks of escalation following a failure to deter.

Roots of the Problem: New Departures in Theory

We begin with concepts. The theory of international relations provides benchmarks to frame the virtual weapon's revolutionary effects on security affairs and the difficulties that hinder the prevention and limitation of its use.

Most theorists of international relations start with an ideal type of a "system" that includes an assumption of (1) units—a broad consensus that states (sometimes only large ones) are the principal and irreducible actors to which all other agents, domestic and international, are subordinate; (2) purposes—the existence of common elementary goals such as the preservation of order that moderates the rivalries of these sovereign entities, especially the resort to violence between them; and (3) procedures—rules, laws, and institutions that sustain this temperance of behaviour and facilitate cooperation even in the absence of a central authority to suppress the will of the units.

The theory of cyber studies must start elsewhere: the new phenomenon disturbs these familiar notions. The most fundamental point of departure concerns the units. Rarely do acts of private players rise to the level of international security significance; hence theorists customarily ban such agents from their conceptual models. Scholars focus instead on the destabilising effects of technological change on the balance of power among the traditional units—the states. The cyber revolution does not tolerate such preconceptions; the related technology's empowerment of non-traditional

actors erodes our rigid models. Although governments remain the principal players in the cyber domain, they are not alone in acquiring significant attack capabilities. The number of non-traditional players—civilian militias, hacktivists, criminal syndicates, even lone agents—capable of damaging critical computer systems is likely so large as to be inestimable. True, a high-impact cyber event that produces physical destruction or loss of life comparable to a traditional act of war requires—so far as we can tell—the apparatus and resources of the state. Nevertheless the new entrants on the international scene have a proven ability to cause alarming harm.[4] For instance, private culprits have used the new capability to convulse the financial and government affairs of a small nation in peacetime (Estonia in 2007); and to interdict the central bank and communications activities of a country in war (Georgia in 2008).[5] In short, the cyber revolution's most profound disturbances may be its effects, not on the balance of power but on the balance of *players*.

Second, is the new technology's implications for elementary goals—the basic political framework of international anarchy that renders the dealings of states not just a mechanical system of interlocking units but also a "society," albeit a rudimentary one, in which the stakes of conflict are limited.[6] Indeed, governments have shown restraint in the use of highly disruptive or destructive cyberweapons, as demonstrated by the United States' decision not to employ the new capability to disrupt Iraq's financial infrastructures prior to the invasion of that country in 2003 or to disable Libyan air defences in preparation for the air campaign to depose Muammar Gaddafi in 2011.[7] In both cases the restraining factor was one familiar to scholars of international relations: the basic concern for order—an unwillingness to set a precedent for future action that could destabilise the strategic competitions of states more broadly. At the same time, there is an explosion of adversarial cyber activity at a lower spectrum of action, that is, at a level that law and diplomacy recognise as less than an armed

4. On power diffusion in the cyber domain, see J.S. Nye Jr., *The Future of Power*, New York, NY, PublicAffairs, 2011, chap. 5.
5. Analysts have also warned about the potential for a major cyberattack by terrorists—for example, Islamic State, with its state-like resources. See H. Kuchler, "Warning over ISIS Cyber Threat," *Financial Times*, September 18, 2014. On the Estonia cyberattacks, see President of Estonia Toomas H. Ilves, address given at the European Union Ministerial Conference on Critical Infrastructure Protection, Tallinn (Estonia), April 27, 2009. On the Georgia attacks, see U.S. Cyber Consequences Unit (US-CCU), *Overview by the US-CCU of the Cyber Campaign against Georgia in August 2008*, Special Report, US-CCU, August 2009, <www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.
6. The paramount treatment of the international system as a society is H. Bull, *The Anarchical Society: A Study of Order in World Politics*, London, Macmillan, 1977. A more recent study is A. Hurrell, *On Global Order: Power, Values, and the Constitution of International Society*, Oxford, Oxford University Press, 2007.
7. See J. Markoff and Th. Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *The New York Times*, August 2, 2009; and E. Schmitt and Th. Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times*, October 17, 2011.

attack or use of force, ranging from the seizure of military and industrial secrets to the disruption of computer systems at financial institutions and major corporations (more on this below).

Nonstate culprits may repudiate the traditional imperative of states for the preservation of order as it applies to this (and other) domains of conflict. They may exploit the asymmetric advantages that the diffusion of cyber technology confers on them to disrupt the delicate political framework of interstate dealings (or to subvert domestic regimes, with similar effects). Examples of how this can occur are not far to search. Culprits for instance could perpetrate a catalytic "false-flag" event, an attack that crashes one country's computer infrastructures while making it seem that another nation was at fault, thereby instigating a diplomatic crisis. Or else the new entrants may simply misinterpret or misunderstand the intricate requirements of international order (seasoned statesmen fail to grasp them) and act in ways that produce a breakdown of moderation even without wishing to do so.

A third departure concerns procedures: few exist to govern the new arena of competition. States do not agree on a framework of rules, laws, and institutions to regulate cyber conduct between them. Attempts at consensus have been made; none has gone far. The Council of Europe's Convention on Cybercrime—the only notable international treaty on the cyber issue—regulates illicit activity by private actors but it has no jurisdiction over governments and does not cover strategic aspects of their relations. Moreover, a United Nations Group of Governmental Experts has affirmed that the organ's Charter applies to the regulation of cyber conflict—yet there is no consensus on the thresholds for an armed attack or use of force in the new domain, much less an agreement on proportionate responses to them.[8] The customary reluctance of the major units to subject themselves to external supervision limits the appearance of such regulatory devices. But there is also a deeper problem: the inability of the regulatory framework to adapt itself to address the challenges of getting nonstate actors that are not typically considered its subjects to comply with the rules and norms of international society. An intergovernmental regime to curtail the proliferation of offensive cyber artefacts, for example, would not stem their trade among private agents who can acquire the technology in illicit markets.[9]

8. Scholars and analysts have begun to answer such legal questions even as states continue to disagree over them. See M.N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013. On the UN report, see J. Psaki, "Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues," U.S. Department of State, June 7, 2013.

9. On malware markets, see S. Harris, "Black Market for Malware and Cyber Weapons Is Thriving," *Foreign Policy*, March 25, 2014; and "The Digital Arms Trade," *The Economist*, March 30, 2013.

Problems of Deterrence

Let us turn now to the first strategic knot: how to deter. Traditionally an attack is deterred by two techniques, denial and punishment.[10] The virtual weapon spoils the logic of each in important respects.

Deterrence by denial works by reducing the effectiveness of the other side's arms. In the nuclear realm, for example, the ability to repel an attack rested on the development of a defensive glacis capable of nullifying enemy missiles in transit or on the mutual reduction of strategic forces to such a low level that the contenders can protect even against weapons that hit their targets.[11] Neither method of denial is easily attainable in the cyber domain, however. A number of factors complicate the neutralisation of weaponised code in transit: the abundance of possible access vectors that an attacker can employ singly or simultaneously; the sheer speed of the weapon, which can travel the information layer at the speed of electrons; and the difficulties of detecting the very presence of a cyber artefact, even after it has penetrated a computer system's logical environment, because (a) the payload is an intangible with few material properties and (b) it exploits coding vulnerabilities (so-called zero-days) that by definition are unknown to the defender. This last factor is an especially worrisome feature of the new strategic landscape. Permanent intrusion affords a sophisticated attacker the means to deprive the defender of the ability to manage his own defences.[12] Likelier than the defender denying the assailant in transit is the assailant denying the defender *in situ*.

Moreover, the impossibility of reducing the full effects of cyberattack impedes denial by means of redundancy and resilience. Here we must distinguish direct effects (i.e., effects within the logical habitat of the compromised computer system) from indirect effects (those cascading beyond it). The virtual weapon's direct effects are reproducible and measurable. Computer specialists can study them in a controlled laboratory environment provided they possess relevant systems data on the target.[13] Not so

10. Modern deterrence theory emerged out of the nuclear revolution, to which the current cyber revolution is, rightly or wrongly, often compared. See B. Brodie, "The Anatomy of Deterrence," *in* B. Brodie (ed.), *Strategy in the Missile Age*, Princeton, NJ, Princeton University Press, 1958; B. Russett, "The Calculus of Deterrence," *Journal of Conflict Resolution*, no. 7, June 1963, p. 97-109; A. Wohlstetter, "The Delicate Balance of Terror," *in* H. Kissinger (ed.), *Problems of National Strategy: A Book of Readings*, New York, NY, Praeger, 1965; and P. Morgan, *Deterrence*, Beverly Hills, CA, Sage, 1977.

11. See R. Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Propsect of Armageddon*, Ithaca, NY, Cornell University Press, 1989, p. 10. See also G. Snyder, *Deterrence and Defense*, Princeton, NJ, Princeton University Press, 1961.

12. See Kello, "The Meaning of the Cyber Revolution,", *op. cit.*, p. 28.

13. Reportedly the United States simulated the Stuxnet worm's direct effects on a replicated industrial control system before unleashing the artefact into the Natanz nuclear facility. See D.E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, New York, NY, Crown, 2012.

the indirect effects. The reliance of modern society on complex computer systems for core functions of government and the economy, and the interconnectedness between both these systems and the functions they support, mean that a hostile cyber event can produce cascading consequences that affect essential activities across a range of sectors and jurisdictions. These indirect effects are largely unknowable before attack; possibly after it too. Furthermore, the responsibility to protect critical computer systems is unclear and fragmented within and across the public and private sectors. Such divisions in the defence establishment will limit the recuperative powers of society in a cyber emergency. The attainment of redundancy and resiliency will be more difficult than heretofore.[14]

Complications of denial have produced a tendency to deter cyberattack by severe punishment.[15] The equivalence principle represents the quintessence of this preference: it affirms the right of the victim of a major cyberattack to retaliate with conventional—even nuclear—arms.[16] In this way the principle is an attempt to port to the new domain of conflict the classical logic of cross-domain deterrence, or the strategy to counter a threat in one domain by the pledge of reprisal in another. Whatever the means, the technique of punishment is at bottom a psychological mechanism.[17] It works by creating an expectation of penalties that induces the adversary to believe it is in his interest not to attack.

Here the problems begin. The difficulty of attaining credible attribution of the identity and location of an assailant degrades the crucial psychological base of the logic of penalties.[18] The difficulty inheres in the opaqueness of cyberspace, but it is also concerns the traditional sate-centric procedures of international relations. National borders dissolve on contact with malware. Cyberattack sequences almost always traverse multiple

14. On the difficulties of cyber defence, see S. Baker, N. Filipiak, and K. Timlin, *In the Dark: Crucial Industries Confront Cyberattacks*, Santa Clara, CA, Center for International and Strategic Studies - McAfee, 2011; and J. Arquilla, "Cyberwar Is Already Upon Us," *Foreign Policy*, February 27, 2012, <www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us>.

15. A similar evolution in strategic thinking occurred very early during the nuclear era. See B. Brodie, *The Absolute Weapon*, New York, NY, Harcourt, 1946.

16. As one U.S. soldier crudely puts it: "If you shut down our power grid [with a cyberattack], maybe we will put a missile down one of your smokestacks." S. Gorman and J.E. Barnes, "Cyber Combat: Act of War," *Wall Street Journal*, May 30, 2011. See also Defense Science Board of the Department of Defense, *Resilient Military Systems and the Advanced Cyber Threat*, Washington, DC, January 2013. Similarly, a recent NATO report avers that a major cyberattack could elicit a traditional collective defence response. *NATO 2020: Assured Security; Dynamic Engagement*, Brussels, NATO Public Diplomacy Division, May 17, 2010.

17. See P.M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," *in Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington, DC, National Academies Press, 2010, p. 56.

18. On the problem of attribution, see D.D. Clark and S. Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks*, *op. cit.*, p. 25–40.

jurisdictions. Multilateral mechanisms to facilitate forensic investigation in the aftermath of attack are therefore crucial—yet few exist or have proven useful. Bilateral diplomatic tools, such as mutual assistance treaties, are cumbersome in dealing with a scenario that implicates dozens of sovereign districts.[19] Another problem relates to nontraditional players—that scourge whose influence theories of international relations struggle to assimilate. It is difficult to adjust the logic of penalties to the threat posed by private actors. Their motives and interests vary enormously; these may be difficult to discern or interpret. Religious fundamentalists, for instance, are unlikely swayed by calculations of material loss—they are essentially undeterrable. Thus even if the difficulties of attribution were surmountable, the defender may not know the cost structures of all relevant opponents or possess viable means to affect them.

In brief, deterrence by punishment requires a differentiation of assailants and an appraisal of tactics appropriate for depriving each of his objectives.[20] The diffusion of cyber technology in modern society multiplies the universe of possible assailants; hence it multiplies the deterrer's anguish.

There is however a caveat to the attribution problem. The greater the sophistication of a cyberattack, the lesser the difficulty of authenticating its source. For the most advanced offensive operations, especially those with destructive direct effects, require lengthy planning and enormous resources to mount. This reduces the number of possible instigators of a calamitous cyberattack. Yet the identification of the perpetrator in such a scenario will rest largely on inference, which reduces the degree of certainty of the attribution—and thus diminishes the legitimacy of the reprisal too.

Even if it is effective in preventing a high-spectrum attack, the doctrine of equivalence creates its own problems. Chief among these is the "stability-instability" paradox (to purloin a term from nuclear strategy): the policy of severe reprisal reduces the chances of a catastrophic cyberattack, but in the absence of options to punish lower-spectrum action it erodes the expectation of reprisal to such attack. Thus the risk of a high-impact event diminishes even while that of lesser aggression rises. The paucity of major cyber events alongside the explosive growth of low-spectrum activity gives credence to this paradox.[21]

---

19. The Estonian cyberattacks for example crossed more than one hundred jurisdictions.
20. One British official explains: "[R]educing vulnerability requires an understanding of people's behaviors as much as it does network topology." Quoted *in* N. Harvey (MP), "Meeting the Cyber Challenge," speech delivered at Chatham House, November 9, 2010.
21. The U.S. Department of Homeland Security, for example, recorded 50,000 hostile cyber incidents against American computer systems in the period between October 2011 and February 2012. See M.S. Schmidt, "New Interest in Hacking as Threat to Security," *New York Times*, March 13, 2012.

Resolution of the challenges of denial and punishment is not in prospect. Complications of cyber defence are not diminishing; they may even grow larger. The more computer systems gain in complexity and connectivity, the greater the defender's burden in protecting them. And while the fear of reprisal may induce the most capable contenders—think of the United States, Russia, China, and Britain—not to exploit the defensive gap for maximum destructive effect, the resulting stability-instability paradox generates conditions for lesser offensive action.[22] To be sure, the doctrine of equivalence will not restrain an adversary bent on a showdown. It may however tempt an opportunistic opponent to explore the unspecified upper reaches of "equivalence" in a way that precipitates an unwanted crisis on the basis of miscalculation or misinterpretation of the defender's threshold of tolerance. Therefrom stems a new problem: how to manage a cyber exchange following a failure to deter.

Problems of Conflict Management

Absorption with the logic of penalties complicates the resolution of this puzzle. It creates forces for an accelerating crisis should a showdown in fact occur. The failure to prevent attack may induce the victim to overdeliver on the promise of reprisal to restore the credibility of the deterrent. This sets conditions for an intensifying spiral of response and counterresponse.

The problem is in part one of procedures. Scholars and public officials have called for the application of core principles of *jus in bello*, such as proportionality, to cyber conflict.[23] Yet what is a "proportional" response to a major disruption of computer systems and networks? What, in cyberspace, is the analogue of a conventional strike? If it be the loss of life or the destruction of material property, the traditional criterion of interstate violence supplies a clear answer. The virtual weapon, however, challenges this cherished benchmark of security studies scholars. Consider a hostile cyber event that interrupts stock trading platforms. The action causes no loss of life and no material destruction. Nevertheless it may erode public confidence in a nation's entire financial system.[24] What price for such a severe yet intangible (at least on military terms) loss? The quest for a satisfactory answer raises peculiar dangers. In the absence of known or agreed "conversion" tables to guide the application of equivalence, it is possible

22. Another force of restraint among the large powers may be *deterrence by entanglement*, whereby the unknown risk of "blowback" arising from the interconnectedness of computer systems discourages their disruption.
23. See J.A. Lewis, "A Note on the Laws of War in Cyberspace", Center for Strategic and International Studies, April 2010.
24. Russia for instance may have planned an offensive operation to disrupt the Nasdaq exchange in 2014. See M. Riley, "How Russian Hackers Stole the Nasdaq, "*Businessweek*, July 17, 2014.

that the punished party will perceive the conventional reprisal—whatever its form—as excessive.[25] The resulting grievance may induce a further unreasonable counterresponse, possibly in kind. And so on: what began as a contest in cyberspace intensifies into a familiar clash of militaries.

Let us nonetheless assume it will be possible to define a spectrum of intensification that prescribes precise graduated steps in a conflict—a rational scheme of escalation control for the cyber domain, one similar to the framework Herman Kahn expounded for the management of nuclear war.[26] Procedures to implement it may not exist. In a cyber conflict, the decision to restrain, scale down, or terminate the exchange will be ineffective by itself unless the contenders understand it. Thus even if the parties share the elemental imperative for the sustenance of order in their strategic dealings—especially during a situation of armed tension—mechanisms to convey the intention may not exist. There are no proven or established procedures to signal the desire to limit the intensity of a cyber showdown. What is a "limited war" in the new domain? What counts as proof of the "cessation of hostilities"? What constitutes conflict "termination"? The answers are not clear—if the questions have at all been posed.

But that is not all. There are other dangers of misinterpretation of the new technology. Under conditions of dire emergency, even unoffensive behaviour can appear menacing. By definition, exploitative cyber artefacts do not seek to degrade the operations of the target computer system; their purpose rather is to seize privileged information. But from the defender's perspective, this fine tactical distinction may not be apparent. If the seized data is systems relevant, the opponent can use them for purposes of industrial espionage or else to design weaponized code.[27] Valid as the distinction between cyber "attack" and "exploitation" may be from a conceptual and legal perspective, psychologically it is unreasonable. Doubts about the ultimate aim of cyber exploitation and its potential misconstrual by the defender as the initial phase of attack may lead to unnecessary preemptive action.

Even non-threats can acquire life in this murky domain. It is a starting assumption of cyber defence planning that the most capable adversaries,

---

25. If the United States—the equivalence doctrine's chief exponent—has devised such tables, it has not revealed them. On problems of escalatory ambiguity, see M.C. Libicki, *Crisis and Escalation in Cyberspace*, Santa Monica, CA, RAND, 2012, chap. 4.

26. See H. Kahn, *On Escalation: Metaphors and Scenarios*, London, Pall Mall Press, 1965.

27. Consider the PLA's massive hacking operation of American computer systems that security analysts uncovered in 2013. "We know foreign countries and companies wipe our corporate secrets," remarked U.S. President Barack Obama at the time. "Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air-traffic controllers." D.E. Sanger, D. Barboza et N. Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *The New York Times*, February 18, 2013.

the so-called "advanced persistent threats," for which theorists have an old label, the "great powers," will reside permanently and without detection in a defender's most prized computer systems.[28] In a major conflict, therefore, every significant malfunction in home systems whose cause is unknown becomes a conceivable case of aggression, every intricate cyber artefact of unclear origin or intent a possible case of offensive "sleeper" malware. Here, again, no established procedures exist to reduce uncertainty about the intensions of adversaries or to restore confidence in the mutual desire for a truce.

Another source of escalatory danger—perhaps the most fundamental—relates to the change in the composition of units in the system. The diffusion of cyber capabilities shatters basic distinctions in international relations which traditionally established order and restraint in the contests for security among states.

The dispersion of power means that the interests and purposes of all relevant parties in a conflict may not be known. While nonstate actors do not possess the maximum of capabilities, and thus by themselves cannot inflict the gravest harm, they can bring a preexisting crisis to a boil. An unfolding interstate confrontation will provide incentives and opportunities for private actors—those pests to theory—to act without their government's direction and possibly against its wishes. No one even generally familiar with the Estonian crisis of 2007 can deny that such players can act irresponsibly and disrupt interstate dealings. True, evidence links the hiring of offensive botnets to the Russian security services. But it is not sufficiently realised that the botnet infrastructure itself was operated by criminal syndicates; that attack tools and target information were readily obtainable online; and that the vast majority of attackers acted without the Kremlin's direction or consent. Little could the Russian leadership have imagined or desired that these unsophisticated attacks would prompt Estonian officials to weigh invocation of NATO's collective defence clause. Forces of chaos existed also on the Estonian side. Only barely did the government succeed in restraining its own patriots from striking back against machines inside Russia.[29]

Then there is the problem of state proxies. States, notably China and Russia, are equipping their civilian sectors with a capacity to hit hard with the new technology. The motives for this move are as above. Cyber militias furnish governments the option of plausible deniability in a cyberattack. Furthermore, they provide a means to harness society's technological prowess while avoiding the cumbersome organisational structures and

28. See D. Winder, "Persistent and Evasive Attacks Uncovered," *Infosecurity*, November 21, 2011.
29. Author interview with L. Almann, January 20, 2014.

costs of traditional military formations. But here, again, pressures of instability appear. There is no guarantee that in the midst of a heated interstate conflict the proxies will remain obedient to their parent capitals.[30] What was conceived as a device for states to avoid retribution may in fact become a cause for its invitation.

In sum, the factors of convergence between the world of states and the world of citizens that provide governments political advantages in a cyber conflict are also the factors that can produce a dangerous and unmanageable collision of these two universes.

Last, the arming of private industry poses new risks. Growing acceptance of the right of corporations to use "strike-back" technology against intruders—in essence, to implement their own logics of denial and penalties—raises unknown dangers of conflict instability.[31] Previously companies subjected to hostile intrusion focused on the limitation of damage—reactive defences. Today they increasingly seek to acquire the means to neutralise threats before or as they are carried out—proactive defences, ranging from the insertion of a beacon into attacking machines to their outright incapacitation.[32] Legal conditions for the implementation of strike-back are emerging. In the United States, for instance, the behaviour has met with the tacit acceptance of authorities. Moreover, lawmakers have begun to push for legal frameworks that permit it.[33] The law of nations, however, has little to say about the phenomenon of private actors targeting the machines of other private actors—possibly also of governments—located in foreign jurisdictions. And there are no guarantees that the quarrels of firms will be any less intense than the quarrels of citizens. Firms, far from dampening conflict, may amplify it. They can bring to bear capabilities far greater than the meagre means of solitary or disorganised citizens.

***

Whoever observes the traditional contests of states cannot but discern—beyond the clash of interests and the occasional violence—a social fabric

30. For example, cyber militias in several countries have threatened to use cyberweapons against Russia if it threatened the home nation. See R.B. Andres, "Cyber-Gang Warfare: State-Sponsored Militias Are Coming to a Server Near You," *Foreign Policy*, February 11, 2013.
31. See J. Menn, "Hacked Companies Fight Back with Controversial Steps," *Reuters*, June 17, 2012.
32. In one recent poll of private companies, thirty-six percent of respondents admitted to having conducted "retaliatory hacking." See C. Timberg, E. Nakashima, and D. Douglas-Gabriel, "Cyberattacks Trigger Talk of 'Hacking Back'," *The Washington Post*, October 9, 2014.
33. See comments by Chairman of the U.S. House Intelligence Committee Mike Rogers in "Washington Post Live: Cybersecurity 2014," *The Washington Post*, October 2, 2014, <www.washingtonpost.com/blogs/post-live-live/liveblog/live-cybersecurity-summit-2014>.

of shared purposes and procedures that moderates and regulates interstate dealings. On this backdrop, the analyst's difficulty is in explaining why order and regularity are so absent from the cyber domain. This vast and heterogeneous milieu is not a coherent society: relevant players do not share an identity of purpose. It may not even be a system in a basic mechanical sense: there are few known behavioural laws and regulatory devices to guide the interactions of the relevant units, many of which the conventional apparatus of diplomacy will struggle to absorb because they are not recognised state entities.

The cyber domain represents in short a *pre*-anarchic milieu: it has yet to develop the fundamental quality of orderliness that makes competitions in traditional security realms largely bearable because the contest is in the main regularised and because established mechanisms exist to orient and constrain the contenders.

For the theorist, the peculiar features of the cyber phenomenon present an intellectual difficulty: how to integrate the new danger into political and strategic understandings. The decision maker's difficulty is the reverse and graver: how to adapt and apply outmoded axioms to reduce the measure of peril. These problems of strategy are not unique to our cyber age; previous generations of thinkers grappled with similar quandaries during earlier technological revolutions. But they are amplified by dangerous conditions of strategic instability in the new domain—offense dominance, attribution difficulties, volatility in weapons systems, and power dispersion. Some of these factors weaken deterrence. All of them elevate the risks of an accelerating crisis if deterrence fails.

PE

Mots clés
Cyber War
Cyber Defense
Strategy
Deterrence