Confidence-building and international agreement in cybersecurity

James Andrew Lewis

The global digital network has become the backbone of the world economy and a significant new venue for attack, but there has been little progress in negotiation or dialogue in the broader context of international security. The secure use of cyberspace has become a vital national interest of all states. As a result, states believe that malicious activity in cyberspace creates real risk to their security and they fear that, through misperception or miscalculation, such malicious actions could trigger damaging military conflict. This creates strong international pressure for multilateral agreement, but the discussion is at a very early stage.

Most advanced militaries have cyber attack capabilities and many others are acquiring them. We can regard cyber attack capabilities as just another mode of attack, which like a missile or an aircraft can strike the enemy from a great distance. And like aircraft or long-range missiles, cyber attack can serve both tactical and strategic purposes. Cyber attack will not be decisive; cyber attack by itself will not win a conflict, particularly against a large and powerful opponent. But it does provide military advantage and therefore will be used. How and when it will be used can still be shaped by international negotiation. It remains an open question as to how this new aspect of warfare will fit into the existing framework governing interstate conflict, and where modification or new agreement is required to better manage conflict and risk.

A June 2011 UNIDIR report prepared using open-source information reviewed policies and organizations in 133 states and found 33 states that include cyberwarfare in their military planning and organization.[1] These range from states with very advanced statements of doctrine and military organizations employing hundreds or thousands of individuals to more basic arrangements that incorporate cyber attack and cyberwarfare into existing capabilities for electronic warfare.

Common elements of military doctrine include the use of cyber capabilities for reconnaissance, information operations, the disruption of critical networks and services, for cyber attacks, and as a complement to electronic warfare and information operations. Some states include specific plans for information and political operations. Cyber attack blends the techniques and tactics of electronic warfare and signals intelligence. Cyber attack will seek to disrupt opponent command and control, increasing the Clausewitzian "fog of war" by creating uncertainty and by damaging data and communications. A skilled opponent could damage or destroy critical infrastructure—currently only a few major "Cyber Powers" have the capability to use software

---

James Andrew Lewis is a senior fellow and Program Director at the Center for Strategic and International Studies (CSIS). Before joining CSIS, he worked at the US Departments of State and Commerce as a Foreign Service Officer and as a member of the Senior Executive Service. He was the Rapporteur for the 2010 United Nations Group of Governmental Experts on information Security. His current research examines strategic competition and technological innovation. Lewis received his PhD from the University of Chicago.

commands sent over the internet to cause physical destruction but another 30 states are developing military capabilities and non-state actors will gain this ability as techniques and tools are commoditized.

The military use of cyber attack is not the most pressing problem for international security, but it is linked to other malicious behaviours and, in some ways, it offers the easiest approach to agreement, given the many applicable precedents in international security. The more difficult problems revolve around the use of cyber techniques for intelligence purposes and engagement with non-state actors. Both issues, however, fall within the ambit of state responsibilities (although the linkages are not yet well-defined), meaning that it is possible to develop measures and norms that limit risk. The effect of norms can be reinforced by confidence-building measures (CBMs), actions taken between states to prevent or reduce ambiguity, doubt and suspicion and improve international cooperation. Norms and CBMs to increase stability in the military use of cyberspace could reduce the concern shared by many states over the potential for cyberwarfare. Common understandings among states about cyberconflict increase the likelihood of deterring malicious action and they also allow for tacit communication in the event of a conflict with an opponent. Developing such understandings would make cyberconflict easier to prevent or manage.

There is a shared perception among governments that the threat of cyberconflict is escalating out of control—this explains the explosion of national cyber strategies as more than 70 states develop plans and organizations to reduce risk. There is a new willingness to approach the problem of international cybersecurity as an issue that states can manage using established tools of negotiation and agreement. But translating a shared fear into concrete action has proven difficult. Cyberwar has only recently been considered an issue for international discussion despite more than a decade of breathless media accounts of Pearl Harbors and Armageddons. Before 2000, only a few states had just begun to develop attack capabilities, the potential damage from such attack was limited, and these military programmes were highly classified. This was in contrast to the ongoing and energetic international discussions of internet governance, reflecting both the lack of expertise in the internet community and an inability to perceive potential risks to national interests.

Discussion of international agreement to limit cyberconflict dates from the 1990s, but this discussion got off to a bad start by focusing on a treaty as the means to promote security and stability. Scholars proposed complex legal instruments whose distant ancestor appeared to be the Kellogg–Briand pact of the 1920s, in which states renounced war as an instrument of policy. Also, in the 1990s, the Russian government introduced a draft treaty in the United Nations, in what became a recurring annual exercise that never achieved consensus. While the idea of a treaty attracted support in the General Assembly, it made no progress because of strong opposition from a few western states. The drafts of the treaties were, in any case, unimplementable. How would any state address serious issues in treaty compliance and verification for cyber capabilities? Binding commitments to avoid attack or hostile actions may

be unworkable, if only because potential opponents are unlikely to observe them. Important definitional issues were unresolved, probably because they are unresolvable. A commitment to ban "information weapons" is not very useful if we cannot say what an information weapon is, and efforts to define "cyber weapons" quickly run afoul of the overwhelmingly commercial use and availability of information technologies.

If a cyber treaty makes no sense, neither does a simple extension of the laws of armed conflict into cyberspace. There are areas of ambiguity, including the scale and nature of damage from cyber attack that could qualify as the use of force (an essential prerequisite for action in international law). Some potential uses of cyber attack create uncertainty in meeting the obligations of international humanitarian law for distinction, proportionality and discrimination requirements in identifying legitimate targets. There are yet few precedents for resolving these ambiguities and the result is an increased chance for misperception and miscalculation of cyber actions or the intent behind them that states fear could escalate into more damaging conflict.

These problems continue to hamper international discussion of cybersecurity. In the last few years, however, the situation has begun to improve. While the Internet community and its affiliated organizations remain inadequate as a venue for discussion of the international security aspect of cyberconflict, military and diplomatic agencies in a range of states have identified cybersecurity as central problem. This change reflects the realization in many states that the high-speed global network that forms the basis of cyberspace has become crucial to their economic well-being and national security, and a source of risk to their national security. Haltingly, the international community is moving towards discussion, if not agreement, on the scope, nature and constraints of cyberwarfare.

Alternatives to a formal cyber treaty began to appear as early as 2008. Rejecting formal treaties, these alternatives drew upon the experience of global efforts to control proliferation to develop a generalized model applicable to cybersecurity. Instead of a binding legal commitment, they proposed that states develop norms for responsible state behaviour in cyberspace. Non-proliferation provides many examples of non-binding norms that exercise a powerful influence on state behaviour.

Norms shape behaviour and limit the scope of conflict. Norms create expectations and understandings among states on international behaviour, a framework for relations that provides a degree of predictability in interactions in security, trade or politics. In this context, cybersecurity becomes the ability of states to protect their national sovereignty and advance their national interests. Cybersecurity creates new challenges for international security, as states are bound more closely together and as the perception of "transnational" risk increases, but it is largely a still undefined element in this web of relationships among states.

The idea of a norms-based approach has growing international support and, as in the non-proliferation arena, widespread adoption of norms could pave the way for more formal agreements in the future. In July 2010 a Group of Governmental Experts (GGE) convened by the United Nations Secretary-General was able to produce an agreed report on "Developments in the Field of Information and Telecommunications in the Context of International Security". This was unprecedented; in addition to the inability of a treaty to win consensus, a previous GGE endeavour in 2004 had failed. But the 2010 report itself is only 1,200 words long. In contrast, the first GGE had reportedly produced lengthy and detailed drafts that failed to win consensus. The brevity of the 2010 report was one element of its success (and this is a useful guidepost for future GGEs on cybersecurity), but brevity is also an indicator of the larger problems that hamper building international consensus.

The successful GGE conclusion in 2010 reflected a shared perception among the government experts that the risk of cyberconflict had become a serious threat to international peace and stability and that the absence of international agreement increased the risk of a destabilizing cyber incident that could spiral into a larger and more damaging conflict. The states represented on the GGE were united by a deep concern over the possibility of unconstrained cyberwarfare and how this might escalate out of control into physical violence. They agreed that discussions of norms and rules for the use of force in cyberspace, along with other CBMs, would improve international security and the stability of both cyberspace and the international system.

Winning even limited GGE agreement was difficult. It should be noted however that public accounts from both academic and media sources have largely glossed over significant differences expressed within the 2010 GGE. While the experts agreed on the increasing cyber threat, there was, however, little else where there was common understanding. Some states believe that existing international norms and laws are inadequate for cyberconflict. Other states argue that the existing laws of armed conflict are sufficient for cybersecurity, and are deeply apprehensive of doing anything that would appear to constrain freedom of speech. A central issue, as is often the case in multilateral discussion, is the extent to which states might concede a degree of sovereignty in exchange for greater security.

These differences were not frivolous, but rather reflect deep divisions on how to approach international agreement and very different views on the use of force, the norms that apply to state behaviour, and the sources of risk in cyberspace. In light of these differences, the members of the 2010 GGE were able to reach agreement on five general recommendations for additional action:

> (i) Further dialogue among States to discuss norms pertaining to State use of ICTs [information and communication technologies], to reduce collective risk and protect critical national and international infrastructure;

(ii) Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;

(iii) Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;

(iv) Identification of measures to support capacity-building in less developed countries;

(v) Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25.[2]

These are valuable first steps. Buoyed by the adoption of a consensus report by the 2010 GGE, a few months later the Russian Federation proposed to the First Committee of the General Assembly that a new GGE be established to continue this work. A new group of experts will convene in August 2012. But the discussion of CBMs also faces significant difficulties. Translating the experience of earlier measures applied in other contexts requires effort, if only because the technologies used in cyberconflict are so widespread. The high degree of secrecy that surrounds state cyber activities—a legacy of their signals intelligence heritage—slows any exchange of information. Misunderstandings over the nature of cyberconflict hamper discussion—the frequent resort to nuclear analogies, which are usually inappropriate for cyberwarfare, are examples of this. Much of the open literature descriptions of cyberconflict are imprecise. The combination of a high degree of secrecy and weak research methodology complicate policymaking.

While there is general agreement on a norms-based approach and that cyber norms and CBMs are essential for international security, there is however very little work on specific proposals that would link cybersecurity to the larger international security "system". We still need to define not only an achievable end state for international cooperation in cybersecurity, but also a path to get there. If the objective is to shape state behaviour through a global framework for cybersecurity, there are many intermediate steps yet to be defined. International discussion will need to begin with measures to build confidence and trust.

For some states, the term cybersecurity itself is inadequate. They believe that the issue is "information security". They argue that information is a weapon and that the laws of armed conflict are inadequate for dealing with this new threat to international peace. They have put forward, under the umbrella of the Shanghai Cooperation Organization, a draft Code of Conduct for Information Security intended to shape discussion at the next GGE by blending objectives such as increased law enforcement cooperation with their own concerns about access to information. For the authors of the Code, stability and security are best achieved by giving states sovereign control over the "information space" and by renouncing the threat or use of force in cyberspace.

The fundamental issue for the next GGE is to further elaborate the 2010 recommendations into concrete measures where international agreement could reduce risk from conflict in cyberspace. Accomplishing this requires consideration of both substance and politics, determining both how to achieve restraint and where cooperation is possible now. Common understandings on a range of issues will be essential—these include on how the existing laws of war apply to cyberconflict, on the nature of escalation in cyberconflict and on the responsibilities of states before and during cyberconflict. Shared understandings among states on these topics would help to create an international framework to constrain cyberconflict and to define the potential consequences for differing levels of hostile action. For each of these issues, however, there are ambiguities and, unsurprisingly, there is a wide disparity of views among key states on the nature of the problem.

Challenges

Any future agreement will need to find ways to deal with broad areas of disagreement. There is no agreement on the thresholds for cyberconflict, particularly the key threshold of what constitutes the use of force in cyberspace and justifies the use of force in response. Perhaps most importantly, there are no shared views on the responsibilities of states in cyberspace. This is an unstable environment.

In part, this reflects differing assessments of the sources of risk. Some states see information as a weapon and as much an element of cyberwarfare as "hacking." When a state says that information is a weapon that could be used against them, they are serious—free access to information is seen as a threat to the regime's stability and survival. That this threat is not intentionally (or consistently) directed at them does not lessen it.

The treatment of information is directly linked to the issue of how states will expand sovereign control in cyberspace. The existing governance model, which depends on an almost tribal assembly of stakeholders in various frail institutions, is inadequate for the security and stability needed for a key global infrastructure. Many governments, finding the current situation intolerable, are exploring where it is appropriate for them to increase their role, to reduce risks to their economies, public safety and national security created by a weakly governed internet. The turbulence over internet governance, as states extend sovereign control into cyberspace to protect their national interests, will complicate reaching agreement on norms for international cybersecurity.

There is a wide disparity of views on how to address the problems of cybersecurity. What kind of agreement (implicit or explicit) is needed, what form these agreements should take, their scope and even their venue remain largely undecided. There is agreement that cyber activities are a legitimate military activity, but no agreement on the rules that should apply to it. There is an ambiguous relationship between cyberwar and espionage. This ambiguity increases the

risk of miscalculation or escalation of cyberconflict as there is only a fine line between breaking into a computer to spy and breaking in to attack.

There are key areas of ambiguity in the applicability of existing laws of armed conflict to cyberconflict, including the treatment of third party sovereignty and the amount and nature of damage from cyber attack that could be interpreted as the use of force. Some operational issues, such as the degree of prior assessment needed to meet the requirements of international law for distinction, proportionality and discrimination requirements in identifying legitimate targets, are also unclear. There are as yet few precedents for resolving these ambiguities. While a new GGE might usefully review these ambiguities, it would be ill-advised to seek to resolve them given the limited chance of reaching agreement at this time.

Obstacles to reaching a multilateral agreement

The immense utility of cyber action will shape any international agreement on cybersecurity. States will not give up this new tool for state power. Cyber attack is cheap and offers strategic advantage. First, the importance of information superiority in warfare and the ability to gain real military advantage from the use of information assets makes digital infrastructures too valuable a target to be declared off limits or for cyber attacks to be renounced. The necessary technologies are either commercial or easily derived from widely available commercial products—a laptop computer, an internet connection and a few computer programs. We cannot control the "precursors" for assembling these "weapons". They are cheap, small, portable, easy to conceal and, for sophisticated programmers in or out of government, easy to construct. Special purpose tools for cyber attack are widely available on thriving cybercrime black markets. It is unlikely that any state will renounce the use of cyber attacks.

Nor would a treaty that excludes certain targets from cyber attack make sense. Existing laws of war already define safeguards and limitations on (but do not ban) attacks on civilian targets. We cannot expect more for cyberspace. An alternate approach could be based on non-proliferation, where states developed multilateral norms that define responsible behaviour. The simplest norm would extend existing law and practice to say that a state is responsible for the behaviour of those on its territory—this would constrain the use of proxies and "patriotic" hackers.

Second, action in cyberspace has been an immense boon to espionage. The close linkage to espionage makes states reluctant to discuss or even admit they possess cyber capabilities, and this linkage also makes it unlikely that they will agree to "ban" first use. A "no first use" commitment could require states to renounce cyber espionage—something they are unlikely to do. Since the techniques of attack and espionage are similar, asking for a commitment not to develop or use cyber tools for penetration of opponent networks is really asking for a commitment not to spy. A "no first use" commitment could even be destabilizing if a victim were to misinterpret an instance of cyber espionage as an attack.

The perceived difficulty of attribution of an attack may encourage some states to believe that they can successfully engage in covert cyber action while evading responsibility. A covert attack where the identity of the attacker is unknown has much less political risk. In addition, mercenaries (usually cybercriminals recruited by a state) can launch sophisticated attacks, providing an additional degree of deniability. The difficulty of attribution is often overstated, as it is increasingly possible in many cyber incidents to determine who is responsible using forensic techniques or active intelligence measures, but the perceived attribution problem increases the temptation to use cyber attack.

These problems mean that approaches that seek to limit cyber attack through multilateral agreement on technological constraints face intrinsic and potentially insurmountable difficulties. Cyber attack is a behaviour rather than a technology. Cyberconflict is shaped by covertness, ease of acquisition and uncertainty, and a legally binding convention that depends upon renouncing use, restricting technology, or upon verification of compliance is an unworkable approach for reducing the risk to international security from cyber attacks. An effort to secure an overarching cybersecurity agreement or treaty that attempted to address the full range of cybersecurity issues would be impractical.

An incremental approach

Agreements to reduce the possibility of misinterpretation, escalation or unintended consequences in cyberconflict are a legitimate subject for international agreement and would improve international security. Just as states feel a degree of constraint from norms and agreements on non-proliferation, establishing explicit international norms for behaviour in cyberspace would affect political decisions on the potential risks and costs of cyber attack. The effect of globalization—the deep economic interconnection among states—has if anything increased the need for cooperation among states.

The creation of norms for responsible state behaviour in cyberspace, the expansion of common understandings on the application of international law to cyberconflict, and the development of assurances on the use of cyber attacks would increase stability and reduce the risks of miscalculation or escalation. The single most important norm for multilateral agreement might be a norm that establishes state responsibility for the actions of its private citizens—such a norm could make it more difficult for states to tacitly encourage proxies by ignoring them or denying involvement with their actions.

However, even simple norms face serious opposition. Conflicting political agendas, covert military actions, espionage and competition for global influence form the context for international discussion of cybersecurity. While there is little or no support for the idea of a treaty, and while international efforts now focus on a norms-based approach, the level of distrust among powerful states is too high for easy agreement on norms.

Disparate values and deep distrust shape the environment for negotiation. Fundamental differences over values, despite formal acceptance of universal human rights, means that the initial set of norms likely to be acceptable to many states is limited. Ultimately, increased stability and security in cyberspace will require common understandings among states on their national responsibilities, on how the laws of war apply, where restraint in the use of the new military capability is possible, and where red lines or thresholds for escalation might exist. But there is too much distrust among competitors to move immediately towards global norms for cybersecurity.

This suggests that international efforts should first focus on CBMs as a foundational element in creating stability and security in cyberspace. CBMs, which require agreement on process rather than on values, could be more attainable in the early phase of creating an international framework for cybersecurity. Incremental steps that focus on reaching multilateral agreement on confidence-building processes for transparency and communication —such as increased transparency in doctrine—may be the most productive approach for reaching agreement in the near term.

Judging from recent and valuable discussion at the multinational conference "Challenges in Cybersecurity" (held 13–14 December 2011 in Berlin, and sponsored by the German Federal Foreign Office, Freie Universität Berlin, the Institute for Peace Research and Security Policy at the University of Hamburg and UNIDIR), there is agreement on the benefits of CBMs, although the portfolio of suggested measures is relatively weak. The leading candidates include greater transparency in doctrine, better mechanisms for crisis management, improved law enforcement cooperation and shared understanding on the application of the laws of armed conflict to cyber attacks. Further work to expand and refine confidence-building measures in cybersecurity will be essential for long-term progress.

Notes

1. *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, UNIDIR, 2011.
2. General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/65/201, 30 July 2010, para. 18.