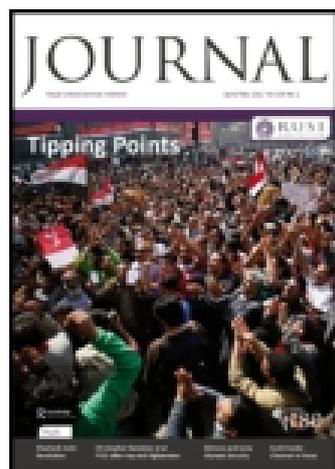


This article was downloaded by: [US Army War College]

On: 01 October 2014, At: 07:07

Publisher: Routledge

Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41  
Mortimer Street, London W1T 3JH, UK



## The RUSI Journal

Publication details, including instructions for authors and subscription information:

<http://www.tandfonline.com/loi/rusi20>

### CYBER-SECURITY THROUGH ARMS CONTROL

Paul Meyer

Published online: 20 May 2011.

To cite this article: Paul Meyer (2011) CYBER-SECURITY THROUGH ARMS CONTROL, The RUSI Journal, 156:2, 22-27, DOI:  
[10.1080/03071847.2011.576471](https://doi.org/10.1080/03071847.2011.576471)

To link to this article: <http://dx.doi.org/10.1080/03071847.2011.576471>

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at <http://www.tandfonline.com/page/terms-and-conditions>

# CYBER-SECURITY THROUGH ARMS CONTROL

## AN APPROACH TO INTERNATIONAL CO-OPERATION

PAUL MEYER

**The risk of cyber-warfare is growing. With a low-level technological requirement, it is a form of warfare that can be prosecuted by military and civilian, state and non-state actors alike. Its anonymity makes it difficult to trace perpetrators, complicating inter-state relations. But cyberspace is not yet an active battleground for cyber-warfare, and could still be amenable to conflict prevention and restraint measures. The time has come to adopt an 'arms control approach' to cyber-security.**

As the global presence and importance of the Internet grows so does concern over its security. Indicative of the official attention cyber-security is now receiving is a statement from the US National Security Strategy released in the spring of 2010: 'Cyber security threats represent one of the most serious national security, public safety and economic challenges we face as a nation'.<sup>1</sup> Cyber-security has two primary facets: the secure use of the Internet and the application of Internet capacities as a weapon in cyber-warfare. There are international security implications arising from both facets, but it is particularly the latter which concerns the global security community. Cyberspace can be viewed as a new 'environment' for security or military activity, just as land, maritime or air environments have been exploited in the past. At the same time, this new 'environment' can be equated with other environments such as outer space or the seabed, which have been the subject of international agreements pre-emptively prohibiting or circumscribing military activity.

At this early stage in the development of governance systems for the Internet, it will be crucial for the international security community to begin to devise a coherent approach for addressing the security challenges posed by this powerful global network. Such approaches could vary from ones based on laissez-faire principles and reliance on national actions, to comprehensive efforts at preventative diplomacy and the development of treaty-based regimes. This article suggests that an approach informed by an arms control model, drawing upon the experience of states in crafting international security arrangements, can prove beneficial in addressing the new realm of cyberspace.

### Challenges of Security in Cyberspace

The security issues raised by cyberspace pose special challenges to those wishing to bring it into a classic international security framework. These special features can be summarised under the following rubrics: actors, attribution, authority and activity. It is useful to

briefly describe each of these features, as the relationships between them must be taken into account when fashioning any system of international security control.

### Actors

A key challenge of cyberspace is that it is populated by both state and non-state actors. An additional problem is that these two categories of users are not readily identifiable. To compare with the aeronautical realm, civilian and military actors are governed by different regimes, operate frequently from separate bases, engage in distinct missions, often use different aircraft and communication systems and apply distinguishing markings. In cyberspace, these 'functionally observable differences' are not present and one cannot readily tell whether a cyber-attack originated from a civilian hacker, a cyber-criminal, or a military or intelligence agency. The cyber attacks on Estonia in 2007, Georgia in 2008 and on the Dalai Lama's network in 2009 are suspected to have been state-sponsored, but no definitive proof of this has been put forward. These attacks frequently involve the



After a massive cyber-attack on key sites in South Korea and the United States, a member of staff at AhnLab Inc reviews an incident log at the Security Operation Center in Seoul, July 2009. Courtesy of AP Photo/Ahn Youn-joon.

'hijacking' of computers of unsuspecting parties in third countries, which further complicates the identification of the real instigators of the attack.

Non-state actors are not empowered to contract international legal obligations or to be held to account for them: international law is premised upon agreements entered into by sovereign states. It is for the sovereign states to ensure that non-state actors within their jurisdiction respect the law, including international legal obligations that have been incorporated into national law. Furthermore, in the context of international security agreements, the focus has normally been on armament and its use, a field in which states traditionally have enjoyed dominance, if not a monopoly. The major weapons systems traditionally subjected to arms control arrangements were usually in the exclusive possession of official armed forces and were frequently of a specialised nature, not replicable outside of state-directed munitions production. In contrast, the 'weapon systems' employed by cyber-attackers can be readily obtained commercially off the shelf. Furthermore, the intended purpose

of these systems cannot be distinguished by their inherent technological features. The computer used to conduct legitimate research one day can be employed the next to implant malware in a targeted system.

#### *Attribution*

As noted above, the challenge posed by the plethora of actors in cyberspace is exacerbated by their anonymity. While monitoring compliance with international security accords has always been a challenge, action deemed incompatible with treaty obligations was normally able to be traced back to a state party to the agreement. This capacity to attribute a violation (or at least an action raising suspicion of a violation) to a state party to an accord can be considered a precondition for concluding an agreement in the first place. It also provides the practical basis for a suitable response to the action in question, whether this is done within or without the scope of the agreement. The verification tools of the International Monitoring System of the Comprehensive Test Ban Treaty Organization (CTBTO) were, for example, easily able to detect

the nuclear tests by North Korea in 2006 and 2009. This enabled the international community via institutions such as the International Atomic Energy Agency and the UN Security Council to take appropriate action in response.

In cyberspace, however, a cyber-attacker can hide himself readily, and even disguise his attack to appear to originate from a third party. The problem of attribution for a cyber-action is clearly one that will complicate any effort at security controls. Uncertainty about attribution will also constrain retaliatory action. As one analyst has stated: 'It would be a very rash political leader who would authorise a counter-attack in cyberspace without being certain that it would strike the right target and not damage a third party'.<sup>2</sup>

#### *Authority*

The designation of which state agency would lead the response to an international cyber-attack would depend on the nature of the attack. In traditional international security agreements concerned with armament and its use, the responsible state agencies are the respective armed forces or national

security establishments. In cyberspace however, a national security lead cannot be presumed. The vast majority of hostile cyber-activity originates with criminal elements, for which law enforcement agencies are normally responsible. A response to use of the Internet by terrorists might entail pooling resources from both the national security and law enforcement communities. The fact that hostile international cyber-activity is not exclusively or even predominantly a national security phenomenon adds a further complication to the development of internationally acceptable approaches for regulating or policing such activity. It is noteworthy that, to date, progress in devising international collaborative arrangements for countering hostile cyber-activity has been confined to anti-cyber-crime initiatives (for example, the 2001 Budapest Convention on Cybercrime originating with the Council of Europe), for which there exists at present the greatest consensus among states in favour of co-operation.

### *Activity*

Hostile international cyber-activity, as already noted, can be perpetrated by state or non-state actors. Even within the sub-set of state activity there is a major distinction that can be made between actions designed to disable or destroy cyber-capacities of the adversary, and those limited to penetrating and exfiltrating data from the adversary's system. These two separate objectives have led to the coining of the terms 'cyber-attack' and 'cyber-exploitation'. The different functions also relate to the interests of separate elements within a state's national security apparatus. The destructive cyber-attack is generally seen as a tool of military operations, whereas the covert cyber-exploitation is a technique employed by intelligence agencies in furtherance of their mandate to collect intelligence. While this distinction has a certain functional and bureaucratic rationale, both forms of cyber-activity commence with a clandestine penetration of an adversary's cyber-systems. This fact in turn makes any victim discovering such a penetration uncertain as to its ultimate objective. Is this the first move in a devastating

cyber-attack, or merely a limited reconnaissance of a system's capabilities? Given the differing approaches applied to the military and intelligence realms under international legal frameworks – the former subjected to some control and the latter essentially unregulated – these overlapping but distinct forms of state cyber-activity constitute a further challenge to those interested in developing agreed international practices for governing such activity.

### **Factors in Favour of International Co-operation**

If cyberspace presents some novel and difficult features for the application of co-operative international security constructs, it also has several elements that work in favour of such frameworks. Cyber-security represents a subject of global concern for states as dependence on the Internet grows in both developed and developing countries. While cyberspace has witnessed conflict (and possibly state-sponsored attacks such as those against Estonia in 2007 and Georgia in 2008), it has not yet become an active battleground for cyber-warfare (in the sense of full-scale, offensive operations), and hence may be amenable to conflict prevention approaches. Moreover, offensive military doctrines for cyberspace have not been promulgated, nor is there a powerful military lobby in existence championing offensive cyber-warfare (although this may change with the establishment of the Cyber Command within the US military and eventual reciprocal action by other militaries).

### *Cyber-warfare is an 'asymmetrical' tactic*

The relatively low threshold in terms of investment and technical capacity to mount sophisticated cyber-attacks renders cyber-warfare an 'asymmetrical' tactic that can help 'level' the battleground against a militarily superior adversary. This strategic reality can encourage more-developed states to seek diplomatic alternatives to the weaponisation of cyberspace and to the institutionalisation of cyber-warfare. The same logic can of course lead those

states perceiving themselves to be in a strategically disadvantageous position to retain this military 'equaliser' and resist constraining their cyber-capacity through international arrangements.

In this early stage of international consideration of cyber-security it may take an initiative on the part of a leading cyber power to overcome the inertia of national cyber-security establishments and set out a proposal for international co-operation. The work of the UN Group of Governmental Experts (discussed later in this article) may prove instrumental in this regard.

Finally, given that an intensification of offensive cyber-warfare would prompt greater attention to cyber-defences and complicate cyber-exploitation activity, there may be internal pressures on a state to seek international arrangements that would preserve a benign cyberspace in which intelligence collection activity could continue discreetly.

### **Cyber-Attack and the Law of Armed Conflict**

There is considerable attention being given to how cyber-attacks can be addressed within the existing corpus of international law governing armed conflict. It would be convenient if the new technology, represented by the Internet, could be subsumed under an existing international legal framework for security matters. However, as one observer notes:<sup>3</sup>

There is no international consensus on the application of the 'law of armed conflict' to cyber-warfare, most often considered a form of 'irregular warfare'. This confusion stems from both the rapid spread of cyber-warfare and the lack of precedent to guide international regulation of cyberspace intrusions.

A major part of this debate revolves around the issue of whether a cyber-attack can constitute an 'armed attack' as understood under current international law. Related to this question is the issue of what defensive response to cyber-attack would be legitimate and the extent to which the principles of the law of armed conflict such as 'necessity' and

'proportionality' would apply. A major study undertaken by a committee of the National Academies in the United States found 'that the principles of the law of armed conflict and the UN Charter – including both law governing the legality of going to war (*jus ad bellum*) and law governing behaviour during war (*jus in bello*) – do apply to cyberattack'.<sup>4</sup> That said, the same study acknowledged that 'the legal analysis in any given situation involving cyberattack may be more uncertain because of its novelty relative to the use of kinetic weapons, and new analytical work may be needed to understand how LOAC [Law of Armed Conflict] principles and those of the UN Charter do or should apply to cyberweapons'.<sup>5</sup>

### *The world may soon be faced with damaging faits accomplis*

While these issues are likely to keep international legal scholars busy for some time, the current lack of clarity concerning the applicable legal regime should not impede efforts to develop collaborative security arrangements. Diplomatic initiatives aimed at preventing cyber-warfare, or at least curtailing its most destabilising elements, can and should be activated. In the absence of some proactive diplomacy to address the cyber-security issue, the world may soon be faced with damaging *faits accomplis* and precedent-setting incidents of unconstrained inter-state cyber-conflict. As has often been the case in international security diplomacy, preventative strategies with respect to new threats prove a more efficient and effective means of countering them, than permitting these threats to develop and then retroactively attempt to constrain them. The devastating potential of cyber-warfare should prompt early consideration of how best to control this new armament. In the words of a 2010 *Economist* leader: 'As with nuclear and conventional arms control, big countries should start talking about how to reduce the threat from cyber-war, the aim being to restrict attacks before it is too late'.<sup>6</sup>

### **Past Arms Control Models**

In devising co-operative security responses to the emerging threat represented by cyber-warfare, policymakers can draw upon extensive experience with arms control. In this context, arms control is understood broadly to constitute inter-state arrangements governing armaments and their deployment or use. The inventory of past arms control models is wide and flexible enough to accommodate the specific challenges of cyberspace. For the purpose of this discussion, one can speak of two broad categories of arms control: 'prevention' and 'regulation'. 'Prevention' is understood to comprise measures aimed at preventing (or prohibiting) certain behaviour, whereas 'regulation' denotes measures aimed at controlling that behaviour and/or a capacity associated with it. Underneath each of these broad categories, one can distinguish between political and legal commitments. The former represent political engagements on the part of the states that make them, and the latter constitute legally binding obligations normally entered into via an international agreement or treaty.

Prevention-oriented arms control has normally been applied in conditions where a new threat or capacity has been identified, but has not yet been realised or is judged peripheral to the actual security requirements of a state. The Outer Space Treaty of 1967, for example, prohibited the placement of weapons of mass destruction in outer space and the militarisation of the Moon and other celestial bodies. The Seabed and Environmental Modification treaties of the 1970s similarly precluded certain locales or actions for military activity that states had no priority interest in exploiting. Agreement to exclude these marginal areas or activities enabled the protagonists to concentrate their competition in the primary international security fields.

A variant of these prevention strategies dealt with known weapons for which there was a consensus in favour of their elimination, either for reasons of strategic efficiency or humanitarian imperatives. The Chemical Weapons Convention, Biological and

Toxin Weapons Convention and more recently, the Ottawa and Oslo treaties banning anti-personnel landmines and cluster munitions respectively are examples of this type of treaty. In some cases, the prohibition was achieved only subsequent to agreements on preliminary steps. For example, the Comprehensive Test Ban Treaty (1996) prohibiting any nuclear explosive test was the culmination of three decades of efforts to preclude nuclear testing in certain environments (for example, the Partial and the Limited Test Ban treaties). Given the strategic significance of a total prohibition of a weapon system or action, these commitments have usually taken the form of legally binding instruments. Political measures have also been resorted to in some cases as an engagement to refrain from a certain action. The 'No First Use' pledges of nuclear-armed states, as well as more recent pledges not to place weapons into outer space, are examples of this form of political commitment.

Regulation-oriented arms control has tended to be utilised when certain weapon systems have already been incorporated into state arsenals and military doctrines, but where a mutual interest exists in controlling destabilising increases or deployments. The bilateral strategic nuclear arms reduction agreements between the United States and the Soviet Union (later Russia) and the multilateral Conventional Forces in Europe (CFE) treaty are major examples of this type of accord. Sometimes both preventive and regulatory elements are incorporated into the same agreement. The Anti-Ballistic Missile Treaty of 1972, for example, precluded all basing environments with the exception of the fixed, land-based mode for the anti-ballistic missile systems regulated by the treaty. Generally, political actions such as confidence-building measures (CBMs) or 'codes of conduct' have had greater scope in the regulatory approach to arms control. They have frequently provided the initial stage of a trust-building process which is subsequently crowned with a treaty. In a European context for example, the political CBMs under the Helsinki and Vienna Documents regulating conventional armed forces facilitated

the eventual negotiation of the CFE treaty, including its mandatory provisions for notification and inspection. Action on the small arms and light weapons issue in the UN context has been characterised by various political commitments undertaken by states at the global and regional level, while preparatory work is under way on an arms trade treaty.

### *Political actions have had greater scope in the regulatory approach*

'Codes of Conduct' have often been advanced in security contexts where a consensus in favour of more stringent or mandatory measures is absent. They have also been deemed suitable alternatives in situations where the capacity to monitor compliance is not at a level commensurate with entering into a treaty obligation. The Hague Code of Conduct concerning ballistic missiles is an existing case in point. Further examples of this approach include the various proposals for codes or 'rules of the road' governing outer space security which have been advanced by states and NGOs in the UN context. While there is considerable flexibility evident in the current array of arrangements, there is also the reality that coming to a meeting of minds on which one to apply becomes more complicated as the number of parties to the understanding increases.

### **What Form and Forums for Cyber-Arms Control?**

What are we to conclude about the prospects for cyberspace diplomacy from this brief review of the existing inventory of arms control measures? The cyber-security challenges discussed earlier suggest that efforts at applying treaty-based arms control may prove premature, given the problems of attribution and the still-unformed nature of cyber-security doctrine. The lack of defined strategies, transparency of operations and verification capacity, as well as the inherent length of the treaty-

making and adoption process, render legally based arms control problematic for addressing cyber-security threats.

### *Bilateral interaction can be invaluable*

The goal of preventing or moderating cyber-warfare, however, can probably be advanced through carefully crafted political measures. Such measures could seek to increase transparency and build confidence concerning cyber-security intentions. They could also serve to articulate a code of responsible behaviour for states in cyberspace. Initial efforts at developing such CBMs might best be launched in bilateral channels involving the military or security communities of states with developed cyber-capacities. Discussing emerging doctrines and operational concepts can serve deterrent functions, but can also provide a basis for identifying mutually beneficial arms control options. Even just the process of bilateral interaction can be invaluable in clarifying misperceptions, fostering understanding of respective approaches and laying a basis for eventual co-operation. Unfortunately, it would appear that other political or strategic factors have worked against the initiation of such cyber-security dialogues between some of the key states concerned (such as China, Russia and the US). It will be important for decision-makers to ensure that such cyber-security confidence-building channels are not ignored, especially when levels of mistrust are so high.

In addition to the bilateral track, there is considerable scope for multilateral measures of confidence-building, both at the regional and global level. At a basic level, issues of cyber-attack and defence should be discussed at meetings of international security organisations. It is time to support transparency exercises that would illuminate military doctrine and strategic thinking on the emerging cyber-security agenda. Research and development of verification techniques could be encouraged, given the need to resolve or minimise the problem of attribution. The capacity to identify

the true origin of a cyber-attack will continue to be a chief requirement for policing cyberspace. There could also be scope for national or collective pledges not to engage in cyber-attacks. These political measures, while difficult to verify in practice, could contribute to the building of norms in cyberspace. The principle of 'non-interference', which has been applied to satellite-verification technology in several nuclear and conventional arms control agreements, may be an attractive, initial measure for a multilateral accord. Notification of and invitations to observe cyber-security exercises could prove another vehicle for confidence-building, mirroring what was accomplished in the field of conventional forces previously. Regional security organisations such as NATO, the Organization for Security and Cooperation in Europe, the Organization of American States and Asia-Pacific Economic Cooperation/ASEAN Regional Forum have taken some initial steps of this nature, but much more could be done. The G8 has already been active in countering criminal and terrorist use of the Internet through its Roma/Lyon law enforcement grouping. It has also engaged on non-proliferation issues and could now expand this work to consider cyber-arms control. Alternatively, cyber-arms control could be a suitable subject for the G20 to take up, drawing upon its more diverse set of influential states.<sup>7</sup> The exact content of whatever cyber-security restraint measures are agreed is less important, at this stage, than the fact that cyber-security is recognised as a field for international security co-operation and preventative diplomacy.

While confidence-building in the security realm is frequently best achieved at the regional or sub-regional level, there is also scope at the universal level, particularly given the global character of cyberspace. The Disarmament and International Security Committee (First Committee) of the UN General Assembly has begun to address 'developments in the field of information and telecommunications in the context of international security' and a resolution on this subject has been adopted annually since 1998. At the 65<sup>th</sup> General Assembly session

in 2010, a UN group of governmental experts, established pursuant to an earlier resolution, presented its report on 'existing and potential threats in the sphere of information security and possible cooperative measures to address them'.<sup>8</sup> The report notes that states are developing Information and Communication Technologies (ICTs) as 'instruments of warfare and intelligence' and observes that 'Uncertainty regarding attribution and the absence of common understanding regarding acceptable State behaviour may create the risk of instability and misperception'.<sup>9</sup> The report concludes that no state is able to address these complex and dangerous threats alone, and recommends further steps be taken to build confidence and promote dialogue among states. Reflective of the higher profile cyber-security is receiving, the General Assembly in December 2010 adopted by consensus a further resolution (A/RES/65/41) convening another group of governmental experts in 2012 to continue the study of cyber-security measures.

While other aspects of cyber-security are being addressed elsewhere in the UN system, it will be important for the international security dimension

of this issue to receive appropriate attention by the UN's deliberative bodies. The extent of practical follow-up to the recommendations of the UN group of governmental experts will be revealing as to the priority states attach to international co-operation on cyber-security. Prompt and practical action in the General Assembly promoting responsible state behaviour in cyberspace can pave the way for the development of eventual global arrangements in the UN's negotiating forums.

### *No state is able to address these complex threats alone*

#### **A Call to Action**

The ubiquitous and vital presence of the Internet and the emerging awareness of the potential for catastrophic cyber-warfare should galvanise preventative state action. The novelty of cyber-attack and the heavy mantle of secrecy surrounding state capacities and intentions contribute to heightened levels of concern. This concern is exacerbated

by the current lack of norms specifically relating to cyber-conflict and the absence of a consensus as to how existing norms should apply to this new vector of attack. States and civil society actors that see merit in co-operative approaches to international security need to mobilise now to address the looming threat of cyber-warfare. Notwithstanding the special challenges posed by cyberspace, there are measures available in the existing inventory of arms control that can usefully be applied to meeting the cyber-security threat. Given the inherent rapidity of developments in cyberspace, time should not be wasted in considering how its impact on international security can best be managed. ■

*Paul Meyer is a retired Canadian Foreign Service Officer whose thirty-five year career focused on international security policy. He has worked on cyber-security issues as Canada's Ambassador to the UN and Conference on Disarmament in Geneva (2003–07) and as Director-General of the Security and Intelligence Bureau of DFAIT (2007–10). He is currently a Fellow in International Security at Simon Fraser University, Vancouver.*

## **NOTES**

- 1 The White House, 'National Security Strategy', May 2010, p. 27.
- 2 James A Lewis, *Cyberwarfare and its Impact on International Security*, UN Office for Disarmament Affairs, Occasional Paper 19 (New York: United Nations, 2010), p. 10.
- 3 Rex Hughes, 'A Treaty for Cyber Space', *International Affairs* (Vol. 86 No. 2, March 2010), p. 533.
- 4 William A Owens, Kenneth W Dam and Hebert S Lin (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Research Council of the National Academies, 2009), p. 4.
- 5 *Ibid.*
- 6 *Economist*, 'Cyberwar: It is Time for Countries to Start Talking about Arms Control on the Internet', 3 July 2010.
- 7 James A Lewis, 'Multilateral Agreements to Constrain Cyberconflict', *Arms Control Today* (Vol. 40, No. 5, June 2010), p. 17.
- 8 Report from the 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', United Nations General Assembly, A/65/201, 30 July 2010, p. 5.
- 9 *Ibid.*, p. 7.