Getting down to business

Realistic goals for the promotion of peace in cyber-space

A Code of conduct for Cyber-conflicts

Daniel Stauffacher, Chairman, ICT4Peace Foundation & Former Ambassador of Switzerland
Riccardo Sibilia, Head of Cyber Threat Analysis, Swiss Armed Forces, Switzerland
Barbara Weekes, CEO, Geneva Security Forum

ICT4Peace Foundation December 2011

Getting down to business: Realistic goals for the promotion of peace in cyber-space

A Code of conduct for Cyber-conflicts[1]

Daniel Stauffacher, *Chairman, ICT4Peace Foundation & Former Ambassador of Switzerland*
Riccardo Sibilia, *Head of Cyber Threat Analysis, Swiss Armed Forces, Switzerland*
Barbara Weekes, *CEO, Geneva Security Forum*

[1]See also Op-ed on 6 July 2011 in Neue Zürcher Zeitung by Stauffacher, Sibilia and Weekes, calling for a code of conduct for cyber-conflicts (http://ict4peace.org/?s=nzz)

Cover image courtesy http://whartonconsultingconference2011.org/wp-content/themes/awake/images/activation/staged.jpg

Introduction

In addition to environmental concerns, financial instability, conflict, poverty and natural disasters, nations around the world are currently facing another challenge that is here to stay: an invasive, multi-pronged and multi-layered threat, a modern day arms race without visible weapons or attributable actors, characterized by an escalating number of attacks both on and off the radar. The stability of our networked global system and the proper functioning of our countries, cities and daily activities, rely on the Internet. Critical infrastructure - including transport, transport security, nuclear power plants, electricity, communication networks, oil pipelines, and financial institutions - has become a clear target for cyber attacks, with potentially devastating consequences for humankind. The international community is not doing enough to prevent an on-going escalation of cyber conflict.

Given its critical role, and in the interest of providing a safe and secure environment, the Internet should be treated as a global common good. The Internet has triggered an explosion of innovation, entrepreneurial spirit, communication, business activity, economic growth, social networking, and exchange of ideas, but is now at a point where an additional layer of security is needed. Tackling a threat to this mainstay of modern society requires a global effort, a concerted open dialogue to find common ground and solutions.

This has proven not to be an easy task- despite countless international conferences, initiatives and meetings we have seen little real progress in developing an effective international response to cyber-threats. The problem is unwieldy, complex and the very nature of the attacks make it difficult to find common solutions. Cyber-attacks are anonymous and can be state or non-state controlled. It is almost impossible to achieve verifiable and provable attribution of who is attacking.

Cyber-attacks are also difficult to detect, persisting in some cases unnoticed for many years, and, in addition, they offer the attacker the possibility to attribute the attack to a third party. Cyber-attacks are instantaneous and global; data packets can reach the entire world in less than half a second. We are facing a new type of conflict, in which it has become easier to attack than to defend.

What makes cyber-security unlike any other national security issue is that even the individual citizen is an integral part of the defence system. Education, built-in security and audits actually need to start with the end-user whether this be an individual, SME, Fortune 500, NGO, government, hospital, transport provider, police or the military etc. Each actor in the system needs to be “responsibilized” for his / her actions in cyberspace. Whether this will require some new legislation concerning the responsibility and liability of various players in the system needs to be examined. Should Internet Service Providers be made more responsible for what goes through their networks? Should IT manufacturers be liable when knowingly producing compromised hardware or software? In any other industry this would be standard practice, e.g.

if a car company deliberately sold internally or exported compromised, unsafe, vehicles to another country.

At a hacker's conference in 2010, Michael Hayden "used the opportunity to challenge attendees of Black Hat--thousands of programmers, analysts, and security researchers--to devise ways to reshape the Internet's security architecture. "You guys made the cyber-world look like the north German plain--and then you bitch and moan because you get invaded," he said. "We made it flat. We gave all advantages to the offense. The inherent geography in this domain plays to the offense. There's almost nothing inherent in the domain that plays to the defence.""[2] If this is indeed the case, what options exist to ensure a secure online environment? How can countries, both at a national and international level, improve the security of a global system, at the heart of which is an essential and necessary level of freedom?

National Response

With attacks relatively easy to mount on our cyber infrastructure, it is extremely challenging to find the right approach, and balance, when developing a national framework for responding to a cyber-attack. How to manage the challenge of attribution? Should national policy focus more on defence, deterrence or offensive strategies? What about proportionality and unintended consequences of offensive action in cyberspace? How to balance the need to protect freedom of speech and the creativity of the Internet while at the same time monitoring and controlling specific types of content in the interests of national security?

The first step is to accept that a certain amount of uncertainty, risk, discomfort and damages financial or other is unavoidable. There is no magic solution for this type of multi-layered, complex situation, nor is there a structured paradigm in which all the pieces nicely fit. All users of the system: individuals, businesses, governments, police, militaries, need to analyse or assess strategically the cost and benefit of their respective behaviour and practices. Where is the critical point at which any user has to fundamentally re-think security options, investment in security and willingness to share information? Where is the "*Schmerzgrenze*"? What are or could be the incentives to encourage both responsible behaviour in cyberspace and increased international cooperation?

At the moment, the cost to create an optimal defensive system is extremely high for any organization, in particular when faced with restricted budgets, limited resources and a lack of trained personnel. In the internal competition for resources, cyber-security is not always at the top of the list and is sometimes even seen as a hindrance to operating freely and pursuing

[2]U.S. military cyber-war: What's off-limits? Declan McCullagh, Chief political correspondent, CNET. http://news.cnet.com/8301-31921_3-20012121-281.html#ixzz1XwXHsLDu

primary goals. Government agencies, police and the military have the additional challenge of not being in a position to offer lucrative salaries to attract, from an anyway scarce pool, the best people for the job. Solutions therefore need to be pragmatic and geared to defence, managing risk, business continuity and, in a last resort, offensive action.

It is therefore necessary to pool the resources of different actors to take decisive steps forward. A few issues to consider for different stakeholders when strategically planning their resources and defences are outlined below.

The question of attribution is one of the thorniest issues when trying to bring clarity and apply war logic to the cyber domain, and has been one of the main reasons why the cyber conflict discussion has stalled on both a national and international level. If a nation is unable to identify the aggressor with 100% certainty, then how can it respond in an effective way with a counter-attack or deterrent measures?

The assumption today is that it will be very difficult to ever have complete technical certainty about the origin of the attack. This lack of plausible attribution needs to be accepted in order to move the debate forward, and systems need to be established that work around this uncertainty. There are various ways of approaching this dilemma: 1) work from the assumption that the nation hosting the infrastructure from which the attack occurred should take responsibility, or 2) make the case that there is sufficient evidence, even without complete certainty, that nation X is behind the cyber attacks, even if those attacks issue from country Y's infrastructure. At the same time, all nations can maximize the benefits of being able to operate in an environment where 100% attribution is not possible (e.g. Stuxnet), with little risk of provoking open hostilities. The current situation is such that a nation can advance its agenda, i.e. the nuclear disarmament of Iran, without the use of bombs or real risk of war. Several factors contribute to this situation: 1) the framework for how to respond to cyber attacks is unclear; 2) 100% certainty in terms of attribution is difficult; and 3) the risk and costs of responding via traditional warfare definitely outweigh the benefits.

In addition, trying to prove a certain country's involvement in a cyber-attack is extremely costly, time-consuming and requires the attacked country to expose at least some of it's technical know-how, which in turn reduces it's competitive advantage in this new battlefield. As with any crime, the "burden of proof" process takes place after the damage has been done, possibly in a very long drawn-out forensic process, which does not make it easy to respond effectively in a timely manner. This time discrepancy is particularly difficult to manage in the cyber domain, given the accelerated speed of transactions and interactions. This situation could contribute, in some cases, to increased counter-attacks under the radar, thereby also avoiding open confrontation or hostilities.

The question of the involvement of third parties or non-state actors is extremely complex. One option would be to consider that a country hosting a cyber aggressor should have to take

responsibility for both the actions of its citizen(s) and for attacks issuing from its cyber infrastructure (e.g. a cyber warrior in Country X, not acting on a government mandate, who decides to take down country Y's critical infrastructure). However, it might be difficult for nations to accept this kind of responsibility for activities, which are often very hard to detect, within its cyber-infrastructure. One could envisage instead that nations would have a responsibility to investigate suspect activities, and any attack emanating from cyber infrastructure located on within the state. Depending on the scale of the attack, the aggressor could be punished under national cyber crime legislation (when it exists) but would most likely not be in a position to cover the costs of either the damages or the ensuing conflict. Therefore the involvement of the State is unavoidable.

As in the other domains of warfare, each country has to be prepared for the worst-case scenario in cyberspace, which will require defensive action but may also require the use of offensive action. This means clearly stating a policy of deterrence including defining levels at which a cyber attack will provoke a response. "All redlines and threats must be made credible by decision makers either overtly demonstrating their resolve to act or creating visible mechanisms which would unquestionably force their hands when in extremis. Credibility demands that the defender's physical ability to carry out the retaliatory threat cannot be in doubt." [3]

As a certain amount of "probing" and cyber espionage, not to mention cyber crime, will unfortunately continue to be the norm in the future, it is vital that countries specifically indicate at which point an attack will be considered an "act of war" and what possible responses could be. The US has recently released new guidelines from the Pentagon broaching this topic, indicating that an attack on critical infrastructure could justify a military response. It remains to be seen if other countries will follow the lead of the US, or advance different policies in this regard.

Should deterrence or defence not work, offensive action might be necessary and should not be excluded, as in any other domain of war. In order to prepare for this eventuality, it is important to be aware that the cyber-means to destroy electricity grids, or other critical infrastructure, can easily get into the hands of virtually any nation, groups or individual(s) with the required ability and resources. This means that the number of potential enemies drastically increases in the cyber domain as compared to other domains of war. Many more countries and non-state actors will be able to obtain the know-how to cause significant damage on a cyber level than were able to do so via traditional means such as bombing. Smaller and middle-size countries have increased power in this new order, contributing to an asymmetry in traditional balance of power and superpower thinking. The interconnectedness of global systems means that any cyber attack that affects critical infrastructure or financial systems is not isolated. There is quite a high risk of the aggressor suffering damages both due to systemic linkages but also due to unintended consequences. This in turn may lead to a kind of "cyber cold war", in which a,

[3] Cyber-deterrence between Nation-States: Plausible Strategy or a Pipe Dream?, Jonathan Solomon.

"mutual assured destruction" logic prevails. Cyber attacks by one nation on another, or by organized crime, may simply not be worth it. This logic would not apply to terrorist groups or politically motivated hackers, whose primary goal is mainly destruction.

When developing a national cyber defence strategy, the central role of the private sector in any national or international response should not be underestimated. The private sector owns and operates much of the world's critical infrastructure, including finance, energy, transportation, medical, telecommunications and IT. A well-planned cyber attack on a nation's critical infrastructure could have devastating consequences and many unintended or unforeseen side effects. Therefore, at both national and international levels, private sector-police-military-government working groups need to be set up, allowing for an exchange of information, early warning systems and exchange of best practices about how to manage different threats. There is still a great reluctance in the private sector to share or make public information about cyber attacks due to the potentially devastating effect on a company's reputation and thus its ability to retain customer loyalty and provide a return on investment to the shareholders. This dilemma is directly linked to the cost / benefit analysis of maintaining optimal cyber-security. At the moment it is still considered the lesser evil for financial institutions to take the hit and reimburse customers who are victims of cyber attacks. The amount of damage and lost income due to cybercrime is estimated in the billions. The question is at which point does cybercrime turn into a cyber-attack of national concern? And at which point will banks and others stop reimbursing customers and expect the government to step in?

Both the IT and telecommunications sectors are particularly crucial at all levels of cyber-security and national defence. They provide the systems, applications, software and hardware through which most of the globe's critical activities function. However, of great concern, is the growing distrust of IT manufacturers due to weak points and bugs in software, built-in malware in the hardware and an increasing dependence on infrastructure (mobile networks) originating from certain countries. These built-in bugs and malware may not be easily detected and could pose a serious threat to a nation's security. Ideally, systems should be put in place to ensure that components used for national defence, critical infrastructure and police work are "clean" and trustworthy. Assessments or audits are needed on a regular basis. In some cases, banks have started writing their own applications in order to control at least one level in the system. There are also security benefits in not having standardized operating systems and software, which make it more difficult for a hacker to attack with a "one size fits all" approach. Increasingly, it may be the case that nations, possessing the technological ability, will start to produce their own products in order to ensure the integrity of systems in critical sectors.

In order to lessen the potential for havoc, intentional or unintentional, governments might want to consider regulatory measures in critical sectors. This will be difficult, not least because of the additional costs for the companies in question. Governments will have to seriously consider footing part of the bill to ensure that critical infrastructure installations and systems are properly secured against cyber-attacks.

International Response

On the international level the challenges are similar but require even more extensive cooperation and consensus building. At present, the momentum is toward like-minded countries establishing norms of behaviour and cooperative arrangements. However, the push should also be to find common ground amongst all countries including the big powers, even if initially working with the lowest common denominator. The danger the global community faces at the moment is that there are no guiding principles of how to behave in cyberspace. "If nations don't know what the rules are, all sorts of accidental problems might arise," says Harvard law professor Jack Goldsmith. "One nation might do something that another nation takes to be an act of war, even when the first nation did not intend it to be an act of war."[4]

„We're at a very perilous point where the U.S., among other nations, have very capable cyber-war units that are "preparing the battlefield"--planting logic bombs and trapdoors in each other's infrastructures--and they don't really know what their strategy would be if there were a cyber-war. The result could be an accidental cyber-war or something that's meant to be a preparation that's actually very destabilizing."[5]

Not to be forgotten is that, as every user is aware, systemic breakdown of computer systems can also occur without the intervention of a Trojan, virus or other malware. The possibility of being on the brink of a cyber escalation due to unintended system failure cannot be excluded.

Given the complexity of the issue, and the urgent need to make progress, the focus of the international community needs to be on achievable goals. There needs to be a movement away from discussions about a „demilitarized cyberspace", which, as nice as this would be, is an unrealistic goal to achieve based on historical evidence of humanity's inability to completely disarm in any other domain. There also needs to be a shift away from traditional discussions about non-proliferation or cyber arms control talks in the cyber domain. There are serious flaws with these approaches in cyberspace, most notably that almost all the elements that would be considered "arms" in cyberspace have a legitimate dual-use purpose. "Arms" (e.g. malware, vulnerabilities, backdoors...) can also be hidden and developed covertly, and can be used for the full spectrum of offensive cyber activities, including cyber crime, cyber espionage and large-scale cyber attacks, without any differentiation. Finally, there is also the additional complexity of third parties involvement - how to conduct arms negotiations with non-state actors?

[4] Goldsmith on NPR: Extending The Law Of War To Cyberspace, Harvard Law School Professor Jack Goldsmith http://www.law.harvard.edu/news/2010/09/27_goldsmith.html

[5] Security Guru Richard Clarke Talks Cyber-war, Forbes.com http://www.forbes.com/2010/04/08/cyberwar-obama-korea-technology-security-clarke_print.html

Non-binding Code of Conduct

Further to the ICT4Peace Foundation's call on 6 July 2011, and building on the World Summit on the Information Society (WSIS) in Geneva in 2003, the UN Charter, the United Nations Millennium Declaration on peace, security and disarmament, and International Humanitarian Law (IHL), the global community should consider developing a non-binding "International Code of Conduct for Cyber-conflicts", outlining the key do's and don'ts for nations in cyberspace in times of peace, war, peace support and peace enforcement. The international community also needs to focus its efforts on assessing, adjusting and possibly adding to existing legislation, treaties and laws, both *jus ad bellum (UN Charter)* and *jus in bello* (International Humanitarian Law), which could also apply to the cyber domain.

Most importantly, existing processes, at the United Nations, bilateral arrangements and international discussions and processes, such as the recent Cyber-Security Conferences in London in September 2011 and in December 2011 in Berlin, the Tallinn Manual at NATO's Centre of Excellence, could feed into the development of the Code of Conduct, which would aim to build an even broader consensus. At the UN, most recently, Russia, China, Tajikistan and Uzbekistan proposed an International code of conduct for information security in September 2011. In 2010, the U.S. reversed its long-standing policy position by co-sponsoring for the first time a draft resolution on cyber-security that has been introduced in the UN General Assembly by the Russian Federation since 1998.[6]

The Code of Conduct would define what States, shall do, or abstain from doing when they are parties in a conflict, when interacting with parties in a conflict, and during times of peace. The Code of Conduct would also address the role and status of private companies and organizations taking part in a cyber conflict. Finally, the Code of Conduct could become a reference for internationally agreed definitions for the terms used in this field including cyber-peace, cyber-security, cyber-crime, cyber-espionage, cyber-conflict and cyber-war.

It has proven quite difficult to find common ground due to differing perspectives on the role of government and the Internet and also due to the differing language used by key players. There are also constraints that exist due to differing national approaches concerning the concepts of "freedom of information" vs. "control of information". However the goal should be to find the common denominator in national strategies, policies and legal systems. Of critical importance will be to define what actually constitutes a cyber-attack that could be considered an act of war and could therefore justify a kinetic response.

[6] Maurer, Tim, — Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security, Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

In any case, it would be unrealistic to expect countries to agree to any kind of non-binding cyber Code of Conduct where the freedom to attack, for purposes of national security, is not an option. The right of a nation to self-defence is stated clearly in the UN Charter under Article 51:

> *"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."*

Article 41 of the UN Charter also refers to limitation of means of communication as a possible response:

"The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. ***These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication,*** *and the severance of diplomatic relations."*

The Code of Conduct, or existing international legislation, would also need to consider if some types of cyber-attacks should be banned completely: „Even a formal cyber-war may have rules different from those applying to traditional warfare, Hayden suggested. One option would be for the larger G8 or G20 nations to declare that "cyber-penetration of any (financial) grid is so harmful to the international financial system that this is like chemical weapons: none of us should use them."[7]

In addition, the question of critical infrastructure protection needs to be examined in depth, to ensure the on going functioning of interdependent global systems. Attack limitation agreements relating to specific key sectors could be part of this, as could minimum standards for response time in case of attack, maintenance, cyber-security audits, best practices and business continuity plans.

In addition to this, the international community needs to consider the applicability of existing international humanitarian law (IHL), in particular the Geneva Convention and protocols, to the cyber domain and where they might need to be updated, modified or newly defined. "…Actual State practice has shown that the principal international legal challenges posed by major cyber-attacks, such as those against Estonia (2007), Georgia (2008), and Iran (2010), are not restricted

[7] http://www.cbsnews.com/8301-501465_162-20012127-501465.html

to issues of IHL, but also extend to questions of *jus ad bellum* and the law of neutrality." [8] Dr. Eneken Tikk's Ten Rules for Cyber Security, published in July 2011 constitute an interesting starting point for a discussion on how existing rules and legislation could potentially be applied to the cyberspace[9].

Conclusion

Like with many cross-border and cross-cutting issues in today's world, thinking and action should focus on a multi-stakeholder, multi-layered patchwork of interconnected solutions, overlaid by an international code and/or additions to existing international agreements, treaties on jus ad bellum and jus in bello, which could be acceptable for most parties. A certain amount of uncertainty and risk will always exist but might be significantly reduced via increased national and international cooperation. A positive by-product of work done toward a Code of Conduct would be to promote neutral discussion of the work and progress done by different stakeholders to gradually raise consensus on key cyber-security issues. A much-needed platform could be developed for discussions to find common denominators, leading to consensus between stakeholders, based on existing instruments and their respective interpretation.

All countries need to be encouraged to adopt cybercrime legislation along the lines of the European Council's Convention on Cybercrime (Budapest Convention, 2001). Nations also need to examine and assess the need for modifying existing laws to address cyber-specific issues. At both the national and international levels, taskforces need to be established including all the key players to exchange information, provide early warning and explore possible solutions to existing or future challenges.

Nation states need to push the international cyber-conflict agenda ahead, placing a priority on cyber diplomacy both at multilateral and bilateral levels. In parallel to a Code of Conduct and possible modifications of existing laws, bilateral "attack limitation" agreements should also be pursued on a sectoral basis to protect key critical infrastructure installations. The cloak and dagger erosion of trust currently taking place within countries and between countries at the highest level needs to be stopped through increased transparency and trust building. Cyber-cooperation and cyber diplomacy should become the norm. This means increased investment in training, capacity building, development assistance and multi-jurisdictional legal expertise.

[8] Cyber-Operations as a Means of Conflict: Mapping of Current Instruments and Initiatives and Analysis of Principal Challenges to International Law, Nils Melzer, 2011, Page 30.

[9] Ten Rules for Cyber Security. Dr. Eneken Tikk, Article first published in Survival: vol.53 no.3, June-July 2011, pp. 119-132, (see also Addendum at the end of this paper below).

Finally, while cyber-security is critical, and the rights of the citizen and user to live and operate in a safe environment is of the utmost importance, any solution should not diminish the freedom of the Internet, or impede the hugely enriching role it has in our society.

****

Addendum to footnote 10: Ten Rules for Cyber Security, Dr. Eneken Tikk, Article first published in Survival: vol.53 no.3, June-July 2011, pp. 119-132.

The Territoriality Rule
Information infrastructure located within a state's territory is subject to that state's territorial sovereignty.

The Responsibility Rule
The fact that a cyber attack has been launched from an information system located in a state's territory is evidence that the act is attributable to that state.

The Cooperation Rule
The fact that a cyber attack has been conducted via information systems located in a state's territory creates a duty to cooperate with the victim state.

The Self-Defence Rule
Everyone has the right to self-defence.

The Data Protection Rule
Information infrastructure monitoring data are perceived as personal unless provided for otherwise.

The Duty of Care Rule
Everyone has the responsibility to implement a reasonable level of security in their information infrastructure.

The Early Warning Rule
There is an obligation to notify potential victims about known, upcoming cyber attacks.

The Access to Information Rule
The public has a right to be informed about threats to their life, security and well-being.

The Criminality Rule
Every nation has the responsibility to include the most common cyber offences in its substantive criminal law.

The Mandate Rule
An organisation's capacity to act (and regulate) derives from its mandate.

The **ICT4Peace Foundation** aims to enhance the performance of the International community in crisis management through the use of ICTs that facilitates effective communication between peoples, communities and stakeholders involved in crisis management, humanitarian aid and peacebuilding.

www.ict4peace.org