International Cyber Norms:
Legal, Policy & Industry Perspectives,
Anna-Maria Osula and Henry Rõigas (Eds.),
NATO CCD COE Publications, Tallinn 2016

APPENDIX 1

Cyber Security Norms Proposed by Microsoft[1]

1. Limiting and Managing Escalation of Threats in Cyberspace Through Norms

Cybersecurity norms that limit potential conflict in cyberspace are likely to bring predictability, stability, and security to the international environment – far more than any set of confidence-building measures (CBMs). With a wide acceptance of these norms, governments investing in offensive cyber capabilities would have a responsibility to act and work within the international system to guide their use, and this would ultimately lead to a reduction in the likelihood of conflict.

Conflict is often characterized as one of two discrete states: peacetime and war. In reality, whether talking about cyberspace or the physical world, there is an escalation path from more common (yet still complex) events that occur in peacetime, to increasing activity and incidents, disruptions, emerging conflict, conflict, and, eventually war, as shown in Figure 1. Different legal frameworks apply at these various stages.

International policy work to date has primarily focused on cybersecurity norms as a means to reduce risk from potentially complex cyber events at the national and regional levels and advance CBM efforts at the international level.

1 This Appendix is based on Angela McKay, et al, Microsoft Corporation, *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World* (14 December 2014), http://www.microsoft.com/en-us/download/details.aspx?id=45031. Please note that these recommendations were published in December 2014, i.e. before the 2015 UN GGE report: United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by Secretary-General*, A/70/174 (22 July 2015), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

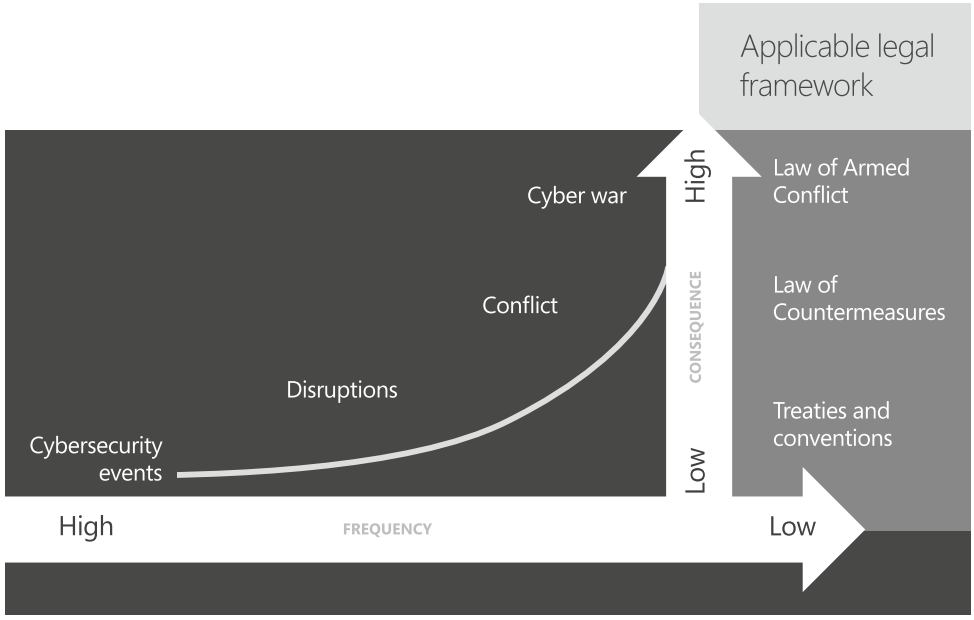

Figure 1. Escalation of cyber events and applicable legal frameworks.

Authorities have paid particular attention to risks and events where there is broad societal agreement on the most significant of issues that face the world – such as armed conflict, nuclear non-proliferation, global resources, and trade. With this alignment on acceptable and unacceptable objectives, actions, and impacts, it seems increasingly appropriate to address cybersecurity risks and events through treaties and conventions. Work to address cyber crime through increased international collaboration is one such example. Another example is the work within the UN, which has looked at a relatively narrow, but vital, segment of cyber conflict for events of extremely high consequence but low likelihood and which would be addressed under the Law of Armed Conflict.

To date, cyber events have not risen to the level of armed conflict. However, while the boundaries between crime and conflict in cyberspace are often hard to discern, events within that space can have broad societal impact, and be challenging to defend against. When existing diplomatic efforts are laid over the spectrum of possible events and applicable legal frameworks, the opportunity for greater development of cybersecurity norms to both improve defense, but in particular limit conflict, is apparent. Figure 2 below illustrates the area where the greatest opportunity for cybersecurity norms exist.

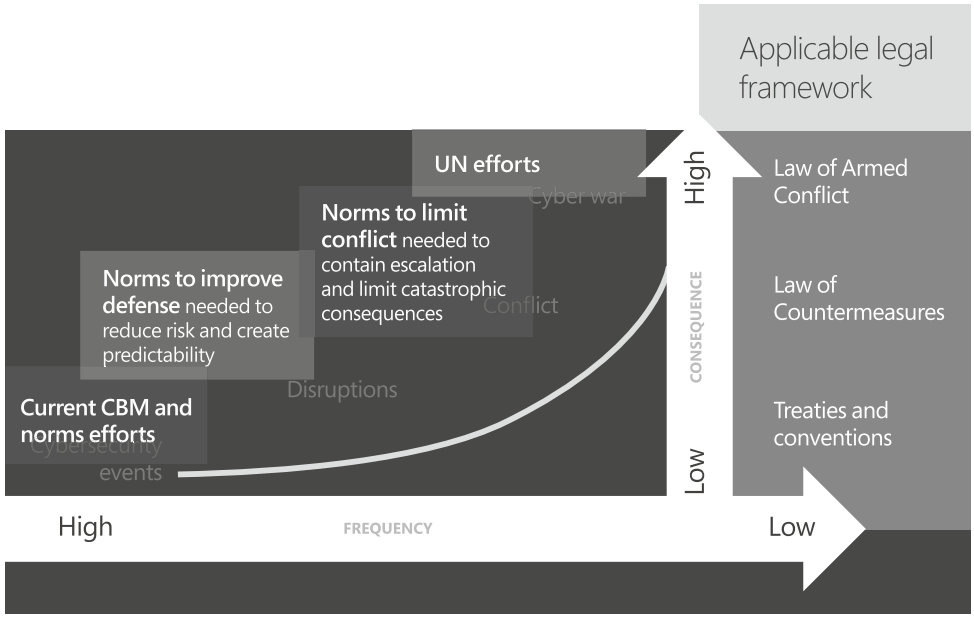

Figure 2. Opportunity space for cybersecurity norms.

2. Six Proposed Cybersecurity Norms to Limit Conflict

In light of the growing number of offensive capabilities, Microsoft believes that cybersecurity norms are needed to limit potential conflict in cyberspace and to better define what type of government behaviors in cyberspace should be 'out of bounds' so that events don't escalate to warfare. These norms should not only be designed to strengthen cybersecurity but also to preserve the utility of a globally connected society.

We believe that if cybersecurity norms are to be effective, they have to meet four key criteria. First, they must be practicable. They also need to reduce risks of complex cyber events and disruptions that could lead to conflict. In addition, they need to drive behavioral change that is observable and that makes a demonstrable difference in the security of cyberspace for states, enterprises, civil society, and individual stakeholders and users. Finally, effective norms should leverage existing risk-management concepts to help mitigate against escalation, and, if escalation is unavoidable, they should provide useful insight into the potential actions of involved parties.

To help catalyze progress on the development of effective cybersecurity norms, Microsoft proposes six norms to limit conflict. The proposed norms are intended to reduce the possibility that ICT products and services could be used, abused, or exploited by nation states as part of offensive operations that result in unacceptable impacts, such undermining trust in ICT; set boundaries for how cyber weapons

are developed, contained, and used; and create a meaningful global framework for managing vulnerabilities. We recognize that norms should not be an objective by themselves. Only if implemented, assessed for accountability, and, as appropriate, evolved, can they drive demonstrable changes in behavior.

NORM 1: States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.

The global technology industry is founded on trust, in that consumers, enterprises, and governments depend on ICT for critical functions. Although the private sector can and does invest considerably in efforts to advance and demonstrate the assurance and integrity of products and services, states have the unique capability to direct disproportionately larger resources to exploit these products or services and to taint the broad ICT supply chains by which they are delivered. Exploiting of commercial off-the-shelf (COTS) products and services – which puts at risk every computer user dependent on that technology, even if that user is of no interest to a government – would be an action with the potential to create unacceptable impacts globally, since the degradation of trust in ICT would threaten innovation and economic security. Sophisticated state-resourced tradecraft targeting ICT companies to place backdoors or vulnerabilities in COTS products – or compromising signing keys to enable government to misrepresent the provenance of software – may exceed the commercially reasonable limits of the private sector operational security and integrity controls. Governments should also refrain from undermining international security standards efforts to benefit their own interests.

NORM 2: States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.

It is well-documented that governments around the world are active participants in the cyber vulnerability market and that they exploit gray and black markets.[2] The Heartbleed vulnerability, discovered in 2014, fueled additional speculation as to how governments stockpile vulnerabilities in ICT products rather than disclosing them to vendors to fix before they are exploited. In April 2014, in response to specific allegations against the US government, the White House published its framework approach to addressing if or when the federal government may withhold knowledge of a vulnerability from the public: 'This administration takes seriously its commitment to an open and interoperable, secure and reliable Internet, and in the

2 'The Digital Arms Trade: The Market for Software that Helps Hackers Penetrate Computer Systems,' *The Economist*, March 30, 2013, http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade.

majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest. This has been and continues to be the case.'[3] The White House further noted that building up a 'huge stockpile of undisclosed vulnerabilities' while leaving the Internet vulnerable and people unprotected would not be in the national security interest of the United States.[4]

Although the White House reserved the right to use vulnerabilities as a method of intelligence collection, this approach does reflect a positive analysis that short-term gains to advance one objective could also create impacts that threaten other objectives, such as economic growth, technological innovation, and trust in government. We recommend that other governments similarly develop and publicly publish their policies on vulnerability handling and that they have a partiality for reporting vulnerabilities to vendors. When doing so, they should adhere to the principles of Coordinated Vulnerability Disclosure (CVD).

NORM 3: States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.

Microsoft recognizes that governments will develop cyber weapons and protocols for their own use. When governments do build them, therefore, they should ensure that they are building cyber weapons that are controllable, precise, and not reusable by others, consistent with the concepts of distinction, discrimination, and distribution previously discussed, to limit the impacts associated with these actions.

NORM 4: States should commit to nonproliferation activities related to cyber weapons.

As states increase investments in offensive cyber capabilities, care must be taken to not proliferate weapons or techniques for weaponizing code. States should establish processes to identify the intelligence, law enforcement, and financial sanctions tools that can and should be used against governments and individuals who use or intend to use cyber weapons in violation of law or international norms. Furthermore, states should agree to control the proliferation of cyber weapons in cooperation with international partners and, to the extent practicable, private industry. Implementing this norm will not only help limit state actions that could have unacceptable impacts but also will help reduce the possibility that cyber weapons could be used by non-state actors.

NORM 5: States should limit their engagement in cyber offensive operations to avoid creating a mass event.

3 Michael Daniel, 'Heartbleed: Understanding When We Disclose Cyber Vulnerabilities,' *White House Blog*, April 28, 2014, http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

4 Ibid.

Governments should review and update their current policy positions with an appreciation for the unintended consequences or impacts in cyberspace that could escalate conflict, incite war or disproportionately harm civilian ICT. During an armed conflict, as regulated by the law of war, any attack must be justified by military necessity, intended to help in the military defeat of the enemy, with a military objective. Furthermore, the harm caused to civilians or civilian property must be proportional in relation to the concrete and direct military advantage anticipated. In other words, the action should be to advance defined and accepted military objectives and should not create disproportional impacts. These strictures can and should be applied to offensive cyber operations. States should recognize that attacks targeting the confidentiality, integrity, or availability of ICT systems, services, and data can have a mass effect beyond any reasonable sense of proportionality and required global action.

NORM 6: States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

Although governments play an increasingly important role in cyberspace, the first line of defense against cyber attacks remains the private sector, with its globally distributed telemetry, situational awareness, and well-established incident response functions. There has not been evidence of governmental interference with private sector recovery efforts following a severe cyber attack, but governments should commit to not interfere with the core capabilities or mechanisms required for response and recovery, including Computer Emergency Response Teams (CERTs), individual response personnel, and technical response systems. Intervening in private sector response and recovery would be akin to attacking medical personnel at military hospitals.

Additionally, governments should go one step further and, when asked by the private sector, commit to assist with recovery and response needs that have global and regional implications. For example, repairing cuts in underwater sea cables often requires permits and cross-border movement of technical equipment or experts, and governments can help ensure that those actions are expedited. Alternatively, a cyber event with large-scale impacts, such as the Shamoon attacks in 2012,[5] could require the rapid movement of hardware from one place to another, the need for international technical collaboration between and among governments and the private sector, and the waiving of legal barriers in times of national emergency to facilitate recovery.

5 Jack Clark, 'Shamoon Malware Infects Computers, Steals Data, Then Wipes Them,' *ZDNet*, August 17, 2012, http://www.zdnet.com/shamoon-malware-infects-computers-steals-data-then-wipes-them-7000002807/.