FRAMEWORKS FOR INTERNATIONAL CYBER SECURITY: THE CUBE, THE PYRAMID, AND THE SCREEN[2]

Thomas C. Wingfield[3], Eneken Tikk[4]

INTRODUCTION

In the myths of ancient Greece, Heracles encountered the evil innkeeper Procrustes, who stretched short travelers and chopped off the legs of tall travelers to fit the fixed length of his guest bed. His name survives today as an adjective describing one-size-fits-all approaches to complex problems. As cyber security has grown into an international and multi-dimensional concern, this article proposes to avoid a procrustean approach to this sophisticated set of problems.

The complexity of cyber incident management has lately been addressed by both national and international regulatory and policy authorities. The national security concerns accompanying trends like patriotic hacking and political context of cyber incidents have forced governments and international organizations to review their existing approaches to internal and external cyber security. The recent examples of policy reviews indicate a shift of national policy towards cooperative, internationally coordinated and layered approach to cyber security.[5]

In this paper, cyber security will be regarded as a domain addressing security aspects of both information assurance and cyber defense, the latter focusing on

[2] The authors wish to express their gratitude to the participants of the 2nd International Cyber Conflict Expert Workshop hosted by George Mason University Center for Infrastructure Protection (GMU CIP) and Cooperative Cyber Defence Centre of Excellence (CCD COE) in April 2009 for discussing and giving valuable feedback on Prof. Wingfield's original concept of the constructs proposed in this article.

[3] Prof. Thomas Wingfield is an Associate Professor at U.S. Army Command and General Staff College teaching graduate-level classes in Operational Law, National Security Strategy, and Joint Operations to field grade officers in U.S. Army.

[4] Ms. Eneken Tikk is a Scientist and the Head of the Legal Team of the NATO-accredited Cooperative Cyber Defence Centre of Excellence. She was a Research Fellow of GMU CIP and is a PhD student of Tartu University Faculty of Law.

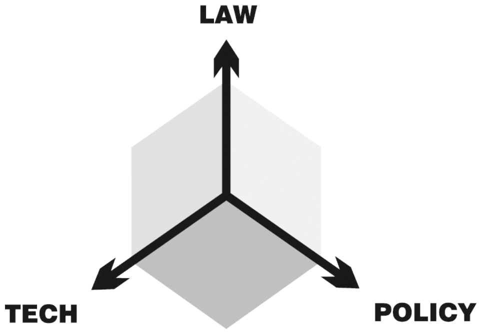
[5] Estonia, after suffering politically motivated cyber attacks in early 2007 and triggering the cyber defense policy considerations by NATO, adopted a new cyber security strategy in 2008. The new administration of the US published a consolidated cyber security policy document in June 2009. Both instruments indicate the need for better international coordination and cooperation in cyber incident management.

military/national security approaches to cyber security. Besides the national security aspect, it comprises other background systems that deal with the reasons for and consequences or activities of cyber incidents, namely the economic, intelligence and policy domains. When put into a legal context, these domains will be related to different legal disciplines covering proactive and response measures of cyber security on national and international levels.

To avoid a procrustean approach to cyber security, it is critical to formulate a framework that addresses all the relevant complexities, but that also provides a sufficient clarity to allow those charged with defending nations and networks to make lawful, coordinated, proactive decisions. This paper will seek to provide initial thoughts for such a framework by introducing the Cube - the three inseparable axes of contemporary cyber security; the Pyramid - a stratified legal response to cyber security issues, and the Screen - the digital environment of relevant expertise and interaction.

THE CUBE: POSSIBLE, PERMISSIBLE, PREFERABLE

It has been said that politics is the art of the possible, but it would be more correct to say that in nowadays world *technology* is the art of the possible, just as law is the art of the permissible, and policy is the art of the preferable. The Cube is simply a name for the highest-level organization for reflecting these three dimensions. Displayed, such a Cube would have an x-axis for technology (the possible), a y-axis for law (the permissible), and a z-axis for policy (the preferable).



Each of these dimensions would have a richly detailed hierarchy of supporting information. The Policy dimension, for example, could be organized into the six categories: diplomacy, intelligence, military, political, legal, and economic (DIMPLE).[6] This DIMPLE construct would allow decision makers in any given area to access the body of information from a perspective that includes as much relevant, and as little irrelevant, information as possible. Determining one's interests and the underlying situation on the axes of the cube, it would be easy to assess what, if any, international legal and policy instruments are there that a policy planner needs to take into account when addressing the response to distributed denial of service attacks under national cyber security strategy.

Further, each area could be organized with an accessible vocabulary and familiar taxonomic structure to add detail to the inquiry, taking into account the cyber incident and envisioned responses in question, *e.g.,* one would be able to narrow the query down to what data protection legal instruments and relevant policy developments address the filtering of network data.

It will be difficult to address all national instruments and approaches in an early model of the Cube. Based on the survey of relevant international instruments, the Cube would indicate the gaps and inconsistencies of international law and policies in the field and, when developed further as a concept at the national level, would also serve as a tool for national policy and law makers to support national cyber security concerns with additional instruments where necessary.

Therefore, the Legal dimension of the first model may be subdivided into internationally addressed disciplines (criminal law, law of armed conflict), and concepts (privacy, freedom of information, telecommunication services, etc). On the national level, the Cube could be much more sophisticated, indicating the source (executive regulations, legislative statutes, judicial decisions, constitutional requirements, recognized international standards), discipline (contract, tort, criminal, administrative), and concept (privacy, terrorism, espionage, fiduciary duty, standards of negligence), with as many subcategories as necessary.

The Technology dimension of the Cube will be based on cyber threat assessment and incident experience. It may reflect the thinking of experts such as Chris Scott of MIT Lincoln Laboratory. Scott organizes technological "attack space components" into attack vectors (user space, kernel, and other), adversary objective (reconnaissance, exfiltration, disinformation, and denial), and attack classes (inject,

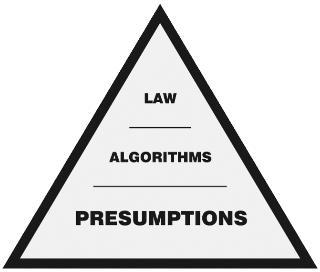
[6] The DIMPLE standard proposed by Prof. Thomas Wingfield suggests that since cyber incident reporting requires the use of technical details, the events need to be described in a manner allowing experts of other relevant fields (Diplomacy, Intelligence, Military, Policy, Law, Economy) to understand the report. This promotes expert discussions in the field and avoids parallel vocabulary on topics of common concern.

byzantine, and life cycle).[7] Another way of subdividing the Technology axis would be to look at the types of cyber incidents of security concern for different nations and international organizations, the proposed proactive and defensive measures (*e.g.*, filtering) and the relevant response levels (*i.e.*, the measures that can be taken at the end-user, organization, ISPs, or national government level, as well as the international engagement necessary).

The very complexity of different options, and the multiplicity of possible organizational schemes, argues for a clear meta-structure such as the Technology/ Law/ Policy Cube.

THE PYRAMID

The Pyramid is a conceptual structure which allows us to organize the process of cyber security implementation as opposed to the substance of cyber security. The three layers (Presumption, Algorithm, and Law) reflect the requirement for three levels of decision-making in dealing with cyber security threats, driven by the speed of operations in cyberspace.



The foundational level, Presumptions, are the black-or-white rules built into a system - an instantaneous if-then decision based on objective criteria and requiring no iterative interaction with the threat. Examples would include automatically disconnecting from a server upon receipt of known malicious code, or fencing a user request from a known hostile source. Presumptions must be drawn very narrowly, in that they will be applied without further reflection or authorization by an automated system. The benefit of presumptions is decision-making and reaction in a matter of milliseconds. It is the equivalent of directing sentries

[7] Chris Scott, *Cyber Warfare: A perspective on Cyber Threats and Technology in the Network-Centric Warfare Battlespace,* presented at US Army Cyber Symposium, September 2008.

armed with nonlethal weapons to "shoot" anyone who comes across wire of their military base near enemy territory, and pursue identification and notification only after the immediate threat has been neutralized. To be lawful and prudent, such presumptions must be applicable to any reasonably foreseeable threat upon which they may have to act. Perhaps the clearest application for presumptions would be as the lawful - and necessary - first line of defense for SCADA systems, whose compromise could threaten the lives of thousands. Gradually, presumptions may also refer to righteous expectations towards managing cyber incidents, such as proper quality and availability of log files to be applied by all ISPs.

The intermediate level, Algorithms, is also carried out by an automated system, but it involves a logic tree to authorize further defensive action. The requirement for additional information will drive an iterative process by which the system will quickly gather the minimum data needed to satisfy cyber "use of force" criteria at cyber speeds. These algorithms are more sophisticated than simple "shoot/don't shoot" criteria, but may still be satisfied by a system quickly enough to react to a potentially crippling attack in time to avert serious damage. To continue our real-world analogy, this would be similar to a sergeant of the guard being told to query potential intruders for a recognition signal before ordering his men to open fire. Computers could be 'instructed' to detect potentially malicious activities and engage additional control towards such signals.

The highest level of the Pyramid, Law, is the most nuanced and the least timely. At this level, humans must enter the decision-making process to make high-stakes decisions based on ambiguous or even contradictory information. There is a requirement for the personal accountability of a human "in the loop," and that person must have the benefit of traditional legal counsel. In these cases, a response would take at least minutes, and probably hours. The benefit is the quality of the final product; the cost is the delay in response that could move a cyber operation from immediate defense to one with sufficient deliberation and planning to appear more offensive in nature. Concluding our real-world analogy, this would be the equivalent of a base commander taking several hours to consult with his legal advisor to determine the appropriate range of responses to civilian protesters threatening to breach the base perimeter and put his soldiers and mission at risk. The broader implications of such a decision would require consultation with higher echelons, and would almost certainly include a political judgment to temper the purely legal range of options.

To secure the responsiveness of the Law level of the Pyramid, clear and accurate legal analysis will be critical. The measures to avoid or manage a cyber incident will ultimately have to be supported by appropriate legal determinations, but these provisions may not always be explicit and easy-to-understand for decision-makers. Therefore, analysis conducted by legal experts will have to take into account the real-life needs indicated by information assurance and cyber defense management authorities and result in conclusions that help other subject area experts apply them in future incidents.

The Pyramid can be constructed upside-down in the sense that the analysis of existing international legal instruments will indicate standards that are most likely applicable in all jurisdictions. Where international instruments are not directly on point, the Algorithms and Presumptions could be based on legal risk analysis, taking into account national best practices and internationally recognized patterns of managing cross-border cyber incidents. However, it bears repeating that since Presumptions are intended to operate automatically and with no immediate human oversight, they must reflect unambiguous determinations of lawful conduct for defense against almost any potential intruder. The challenge will be to maximize available options at all three levels, automating as much of the process as legal precedent, technological savvy and political practicality will permit.

THE SCREEN

The Screen is the final tool we will examine. Whatever theoretical constructs we adopt, and however they are put into practice, they must be put into a form that is quickly and easily accessible to humans engaged in cyber incident management. The Screen is simply the placeholder term for the graphic user interface that will display status and trends, threats and options, probabilities and information gaps.

Much has been learned in the last ten years about presenting high-density information to task-loaded individuals operating under severe time constraints: "all-glass" cockpits in high-performance aircraft, next-generation military command posts, international business networks dependant on highlighting critical data against a high level of background "noise," and even set design for films set in a plausible future, will allow the work of "what if" designers to converge with that of "what is" engineers.

Although perfect real-time knowledge of all cyber threats is an impossible goal, it *is* realistic to do much better at providing a richer, better integrated picture of our cyber security to the technologists, attorneys, and political leaders who will have to collaborate to avert the next cyber attack.

One could think of the Screen as a sophisticated and user-oriented information system delivering the content of hundreds of databases in highly interactive, easy-to-grasp and quickly accessible manner. The visible part of it would be a web space providing well-structured information about the categories represented on the axes of the Cube. It would contain educational materials, lessons learned, and white papers, as well as relevant legal and policy instruments, providing experts and decision-makers with up-to-date and quality instructions on different aspects of cyber security. The Screen could also identify people, organizations, and authorities who could contribute to cyber incident management. As such, the Screen would not only provide a model for decision-making, but also facilitate communication regarding cyber incidents between national governments and subject matter experts.

CONCLUSION

The Cube, the Pyramid, and the Screen represent complementary approaches to clarifying the complexities of international cyber conflict. These tools comprise a system which can be developed incrementally - perhaps initially at the international level. This version could then be made available for comment and elaboration at the national level. With academic and operational feedback, evolving cyber threat assessments and lessons learned from future cyber incidents, the original system could be improved and refined, capturing the complexity and nuance of diverse national approaches.

The three constructs represent the *status quo* of cyber security law and policy, and highlight issues relevant for regulatory and policy authorities at the international, national, and private enterprise levels. Enhanced national models would provide valuable feedback on potential legal issues, responses, and consequences. Over time, these instruments would help clarify gray areas in law and policy as well as identify impractical legal constraints in need of revision on the national or enterprise level.