A Cybersecurity Policy Framework for the 21st Century

[redacted]

Syracuse University College of Law: Cybersecurity Law and Policy
Prof. William Snyder - April 2012

There's no question that cybersecurity is an issue today, and will remain a pressing issue for the foreseeable future. Constructing a clear definition of what is and is not included under the umbrella of "cyber," however, is a much larger challenge. Beyond determining what is and is not contained in this new cyber domains (cyber crime, cyber war, cyber espionage, etc.) we must consider if our current analog equivalent activities and concepts apply to their digital counterparts, and if so, how. Only then will we be able to move forward in a meaningful way towards creating effective cyber policies and guidance.

In this paper, I will lay out a working definition of cyber that facilitates a con extual analysis of component cyber systems with the goal of both increasing sec rity postures and decreasing mis-spent resources, while main aining the fertile ground for innovation that has led us down this path.

Definition and Constraints

On first glance, it seems eas to say what "cyber" is and isn't. It follows naturally form cyber's binary architecture, wh rein everything is represented by either a 0 or a 1, on or off, in or out. This clear cutting of the issue - that omething either is or is not a part of the cyber domain - does not do justice to the difficul y of this distinction, and may actually do a disservice to policy makers and technicians who are navigating these treacherous waters.

While cyber is clearly a separate domain from the physical, the two are tightly interwoven. Today, nearly everything is "online" - cyber impacts all parts of our lives: individually and collectively, personally and professionally. In the developed world, there is no part of today's hum n exi tence that isn't online in some way. Even those who actively eschew technology from a personal perspective are, at some point, impacted.

Considering this new cybe -centric reality, it seems preposterous that a single policy or set of policies that could, in essence, dictate the whole of how we live our digital lives. The scope is too broad, the nuances too great, and before we could make any meaningful progress, we'd be mired in the underlying question of what exactly we are trying to do here.Seeking out a definition that serves as the end-all, be-all is counterproductive in discussions of cyber.

By its very nature, cyber evolves significantly faster than any other tools in the history of mankind, and is able to achieve a scope, scale, and depth unlike anything else. Instead

of looking for a single answer or guiding principle, we should seek to create a framework that is flexible enough to address the difficult questions that will no doubt arise in the future, but grounded in the cultural, legal, economic, and military realities that have always governed society at a collective level.

To facilitate this decision-making process, I propose a model that moves with the context of the challenges and issues, wherein choices of policy and enforcement can be made as needed, utilizing the best available tools to assist the best available people.

A Three Part Solution

In order for this framework to function, significant contributions will have to come from all stakeholders: military and civilian government agencies, including Federal, state, and local, commercial entities, financial services, critical infrastructure, and perhaps most importantly consumer internet.

Additionally, this working group will need to function at the speed of innova on not at the speed of a committee. This model of global collaboration for the greater good is not without precedent: the World Court, the Un ted Nations Security Council and many other organizations have proven we can work together globally to solve difficult and grand challenges. We may need to speed the p ce by o fering the committee some leeway in the form of advice from former United States Supreme Court Justice Potter Stewart's definition of obscenity: "I know it when I see it.

Like obscenity, cyber policy exists n different forms depending on the time, place, and cultural norms. What s considered obscene by the community standards of Dubuque, Iowa may be downright pedestrian in San Francisco The same is true online - what is considered somehow offensive or unwanted by he community at large will change drastically with time and by location Providing this level of flexibility incorporates not just the uses of technology, but the social and cultural norms that develop around digital communities. To ignore this will be to ou peril, as a "one size fits all" approach will surely stifle the potential for innovation and impact.

To further encourage the group to keep pace, members short would serve shorter, one-time tenures of service, say eighteen months, and be selected by nomination of their peers. This group could, in turn, begin tackling difficult problems by taking advantage of the following three pillar solution: Contextualization, Data-Centric Security, and Transparency.

Contextualization

Today, by and large, the push towards security standards has resulted in many lower-grade systems being over-protected, and high-grade systems being under-protected. Instead of protecting our gold bars the same way as our toothbrushes, we need some meaningful yet manageable way to categorize information systems and their functions

to help guide us towards appropriate security controls and considerations. I call this process “contextualization.”

In order to best allocate our limited security resources and personnel, it only makes sense to protect the systems that most need protecting, in the ways that make them as secure as possible while remaining as effective as possible. This means that military, classified, and other National Security systems should deserve different consideration than a set of consumer-grade electronics. Financial systems, the power grid, and others might have different priorities. To do help calibrate these differences, system owners will need to work out their own balance of the classic security triad: Confidentiality, Integrity, and Availability.

Contextualization should take into account several factors, but ultimately hinges on two very important system characteristics: data contents and system capabilities. If ystem owners can create an appropriately balanced blend of confidentiality, integrity, and availability within the context of the system’s data contents and capabilities, th s will represent major progress. To assist in this process, a common set of example data contents and system capabilities should be developed by the proposed oversight organization. In a world where connected systems can all reach each othe , it only makes sense to ensure that we speak the same anguage.

Contextualization will also serve to increase awareness and ould force many system owners to take drastic measures to increase security postu es. One way many system owners will try to achieve this is t rough segregation - keeping their system separate from the public Internet, other machines, environments, or users. Unfortunately, segregation is a methodology that is fundamentally flawed. Segregation assumes that this "secure" or segregated s stem or network is never breached. Once it is, or is thought to have been, the value in segregating and isolating these systems and data is immediately reduced or even eliminated It also makes the input and output of data (a key functionality of any information system) much more difficult, and the ripple effects of being segregated often create more security vulnerabilities than it solves (workarounds to get data in, frustrated users shortcutti g data out, etc.). Instead, if the focus remains on the proper balance of confidentiality and integrity with a retention in availability, segregation should not be necessary for the vast majority of systems.

Data-Centric Security

Once the system level contextualization has been completed for existing systems, our cybersecurity framework should look towards the needs of future systems. Traditionally, security models have focused on users - Role Based Access Control (RBAC) being the classic example. The basic idea of RBAC is that certain users should have certain access to certain data in order to perform certain assigned duties. Typically, this scenario resulted in the creations of standard “users,” who have minimal rights, and “administrators” who have significantly more rights. The problem, however, is that anyone who controls the administrator account (legitimately or otherwise) can control any of the data contained under that role’s umbrella.

One of the most popular responses to this has been to focus on authentication and identification - ensuring that those who are accessing these more powerful accounts are, indeed, the proper people. This has proven problematic in many ways, not the least of which is the difficulty associated with scaling such a model, creating trust between individuals, entities and agencies, and keeping up with user demand, platforms, and applications.

Instead of continuing to focus on the human component, we must move to a data-centric information security model.

Developing security models that are inherent to, and travel with, the data we seek to protect can eliminate much of the concerns around identification and authentication, system integrity, data loss, and many other significant challenges facing today's cybersecurity practitioners.

With the rise of cloud computing and mobile pl tforms, the only question i when, not if, our sensitive commercial and government data will be deployed and subsequently exploited using these new devices and plat orms By focusing our energy n the data itself, we can work to eliminate the challenges posed to data at est and data in transit to and from these platforms.

The computing power of today's mobile devices and distributed clouds is now more than enough horsepower to facilitate a data centric proposal. Dynamic encryption services and other key elements of achieving a true data-centric security paradigm can now easily be performed in the palm of your hand, and scales very well to the cloud and enterprise level.

Transparency

The ultimate tool in helping us make the best possible decisions for how we move forward is transparency: we expend far too many resources re-inventing the wheel in the cyber realm instead of leveraging the work and lessons already covered by many others, both military and civili n, both at home and abroad.

The value of transparency can hardly be overstated. While I understand the mentality behind not wanting to share ones vulnerabilities - you figure you're more likely to get hit if an attacker knows where to hit you. However, you're not the only one facing this problem, and the challenge surrounding vulnerabilities is two-fold: they must first be identified, then mitigated.

Transparency and a "need to share" mentality will not only increase the speed with which vulnerabilities are identified, but also the speed with which remediation techniques are identified. There are several ways in which this could be facilitated. Leveraging the overarching collaborative organization described above, we should work towards is an anonymized or minimally identifiable opt-in system that allows for

knowledge sharing amongst those in a similar position (relate back to the information system categorization) so that best practices and common solutions can be shared, and vulnerabilities identified elsewhere can be mitigated everywhere.

To encourage organizations to contribute knowledge to this collective, a rule should be created to ensure that you must contribute information to be able to access the collective knowledge these contributions represent. While eliminating freeloaders seems impossible in nearly every context, this will significantly increase. Other incentives could be put in place using traditional financial (tax breaks) or regulatory means.

Conclusions and Next Steps

By identifying both who and what should have a seat at the table, fostering an open collaboration while simultaneously allowing ownership, and recognizing the complexity of the problem, there is no reason why we should not be able to solve the grand challenges that cyber presents. Only when we fall into the traps of turf wars, over-classification, and generalize through stereotypes do we reduce our chances of success.

As a living tool, this framework should be freely adapted by those who use it to create and support policies and guidance. The themes contained herein should adapt, as well, with the uses and implications of today's technologies, and tomorrow's. As our physical and digital worlds grow ever closer, closing the policy and guidance gap become that much more important.

I firmly believe that human beings who are capable of creating this world of cyber-enabled possibilities are capable of solving the problems created in the very same stroke. It will not come without resistance, nor will the solutions please everyone. What matters, however, is that we move beyond trying to please everyone, seeking a one-size-fits-all solution, and falling into the traps of complacency and bureaucracy and move forward together as partners in this brave new world.