The Passy Press®
Founded by Benjamin Franklin – 1777
Passy, France

A NOTE ON CYBERSPACE

Cyberspace is the non-physical terrain created by computer systems. Anything related to the internet also falls under the cyber category.

Informally defined, the cyber ecosystem includes the interconnected network of information technology infrastructure, as well as the environment, norms, conditions and people that influence that network, including everyone that uses it.

When the Internet was created, it was intended to facilitate worldwide communications. Security was not a key consideration. Although during that time, encryption of classified or protected information was common - making it likely that the designers would have assumed that the data being transmitted, rather than the internet/system, would have protection. At inception, Internet communication was intentionally open - for good and potentially ill.

The internet soon facilitated automation, enabling operations to be conducted remotely and over great distance. This changed the dynamic since communication could be used to automate control systems (power, dams, transportation, warehousing, etc.) and to remotely adjust the operating environment – again, for good or for ill. At that point, what is now called cyber systems (previously called “network operations”) could be leveraged for communication at all distances, in most activities involving computer interaction and for the purposes of changing physical environments in an automated fashion without presence. Cyber, became a foundation, underpinning and resource that now changes the national, military and economic power dynamic.

Going back a decade or so, USCYBERCOM (United States Cyber Command) and various agencies talked about the evolution of how nation states were leveraging cyber to influence political power and even to facilitate military action. Starting with defacing (changing a website to embarrass or creating propaganda), progressing to denial or interfering with website operations, and finally to destruction (completely taking over or down key websites). These 3 “Ds” were soon applied beyond websites, to the data, trusted processes and even physical (automated) elements of a now connected and worldwide interdependent cyber network.

You have likely read a multitude of stories where hackers infiltrated a network, changing the data to make it useless or untrustworthy, and, then fast-forward, to using cyber to physically

destroy things. Early on, it was nation states that either had expertise or knew where to go to hire, or leverage, the rare experts. However, nations, hackers, activists, criminals, law enforcement, and educators were all equally likely to leverage these capabilities to do “things”. Like a frog being heated up in cold water, we are all now directly affected by this gradual continuum: defacement, disruption, destruction.

Cyberspace is a bit different than traditional environments or domains of land, sea, air and space. While ground, sea, air and space systems can certainly be created and adapted, their domains are determined and limited by the laws of nature. A fundamental difference in characterizing and understanding the cyber domain, is that the cyber domain writ large, as well as the systems that operate in and through it, are created, controlled and can be adapted by man.

It follows that changes in the environments that affect the operation of the physical or natural domains are predictable. Mother nature’s weather conditions, sea conditions, geology, atmospheric and ionospheric affects are largely predictable, and enable some ability to prepare or react. Not so in cyber, where the entire environment is subject to rapid innovation, for good or ill, and with largely unprecedented consequences.

Stability, or changeability has unique implications regarding cyber. Because it can be adapted in days, minutes or micro-seconds, we do not know when someone might be changing it, and we have none of mother natures indications of change. Proactive design controls, security and resilience become paramount now, in a way that was never considered in the early days of the internet designers. If entropy, as a natural state of disorder, is understood for nature, it must be a goal to actively preclude that disorder as we advance cyber design and related policies.

Similarly, traditional boundaries are difficult to apply in a cyber environment. Ground, sea, air and space have an accepted and generally scientifically discernable line of demarcation, a physical divider in their boundaries. Whether it is one of these domains or a sovereign state, or even international waters, there is a definable boundary condition that cannot be easily articulated or enforced in cyber. While some physical boundaries can be defined in cyberspace, like where the servers or data centers reside, those “pieces” of the system can be located anywhere, independent of operations. So, sovereignty and inherent responsibility become problematic. There are no lines of demarcation so it is very hard to box it in or put boundaries around it due to the fundamental differences between cyberspace and nature.

The science behind natural science and cyber are also not the same. Building a satellite or

fifth generation fighter plane needs a really big structure and lots of scientists, which traditionally required a nation state or very large corporate entity. Dissimilarly, in cyber the intention to change things on a global scale does not require the expansive structure, scale or budget of a nation state. Like terrorism, it can be done on a very small scale; but, whereas terrorists have to physically be someplace to blow things up, in cyber that is not necessary. Everyone has access to the capability and the equipment (computer systems) needed for cyber operations. Fewer resources are needed to get in the game. Again, for good or ill.

Another factor that makes cyber different than other domains is how fast it changes, call it speed of change. Although there are great ah ha moments in engineering over time, in say metallurgy and other fields, change in the cyber business is much more rapid.

Nonetheless, cyber warfare and war in the domains of land, sea, air and space are all based on strategic intent and tactical capability. In both, targeting analysis, to learn about what you are going after, is required in order to be effective. In a cyber environment, however, because of the way you have to move, you have to know more upfront. Therefore, the targeting analysis and research component are exceptionally detailed, require unique expertise, are much more dependent on advanced preparation. Additionally, with the changeability of the cyber domain, all the preparation described may be useless in days, minutes or micro-seconds. It is essential to tactical and strategic operations, yet highly fungible. Since you do not control all the pieces in cyberspace and cannot see responses as you go along, you likely have to make predictive decisions and build them in to the operation. This makes it exponentially more complex in a cyber environment, so it takes a long time to do the target analysis, gameplay and campaign plan. But, you execute very rapidly.

Furthermore, in cyber, the assessment is of collateral effect, not collateral damage. Since everything is interconnected, the collateral effect is more complex and potentially far reaching. A traditional test environment is less helpful, because it is not possible to construct at the global scale of the internet and its connective tissue to physical systems.

The power and potential of technology is expanding exponentially through machine learning, big data and quantum computing, for uses, both good and bad. The effect of a major cyber attack against the United States could be existential if undefended.

