The Law of "Cyber-" Prefixes

By LTJG Brandon Karpf, United States Navy

"Cyber-" prefixes have invaded the public consciousness. In the past decade, how often has the greater policy community considered questions such as, "How do we address critical infrastructure cybersecurity?" It is now a reflex to amend traditional technical and policy domains with the term "cyber-" as if the addition has some fundamental meaning. It does not. I propose we discard the "cyber-" prefixes, evaluate contextual domains, and only restore the prefix if such a clarification adds nuance to a specific policy problem.

These "cyber-" prefixes - rarely more than a faddish conflation of jargon - obscure policy problems instead of alleviate them. They serve two unproductive functions. First, "cyber-" prefixes create a false door—a technical barrier between problems and solutions. Instead of revealing solvable issues in a normative domain, this boundary defining language hides well-established solutions behind a veneer of technical complexity. The term cyber carries a technical weight that discourages otherwise intelligent people with salient innovations and creative processes. The prevalent saying, "I'm not a cyber-person" as excuse for not developing an opinion nor intellectualizing a policy problem is counterproductive. These otherwise intelligent analysts retreat from offering their expertise in a field that desperately needs it.

Second, the "cyber-" prefix creates a false pedestal above traditional policy domains and solutions. It leaves the impression that the computer domain presents an organizational, structural, and philosophical anomaly that stands in contrast to centuries of policy development, analysis, and critical thinking. The CEOs of many technology companies hoist this same conceit when they testify before Congress. They claim that policymakers cannot possibly comprehend the innovative complexity of the cyber-domain, that the domain fits within no existing model, and that regulations should not, nay cannot be levied. This mystical belief is false. Unfortunately, this conceit has led to thirty years of languid public policy.

The computer network domain is a system designed by people. While characterized by unprecedented growth, it is still subject to the same first principles as other complex human-created systems such as economics or security. For example, economic first principles show agents respond to costs and benefits, which allows us to shape incentives to influence behavior. Security first principles apply threat analysis to identify vulnerabilities and risk analysis to design controls that mitigate those vulnerabilities. Problems in the cyber domain are subject to the same relevant first principles because they are subject to the same fundamental forces as any human-created system.

Therefore, I propose The Law of "Cyber-" Prefixes... drop the prefix:

> *When someone poses a policy problem, paradox, or challenge by amending a well-established field of study with the prefix "cyber-", proceed as follows: First, drop the cyber. Second, consider the amended statement. If the amended statement has an established solution, apply that solution to the aforementioned "cyber-" problem. Test for viability and salience. Most importantly, drop the cyber.*

For example, consider the initial statement: "How do we address critical infrastructure cyber-security?" The amended statement considers the issue of critical infrastructure security. Defending critical infrastructure is an established field with practiced standards. Applying the same security first principles discussed above reveals that infrastructure security requires access control, security-by-design, security-in-depth, and reflexive evaluation, to name a few. Access control refers to a rational limitation of each person's access based on job scope and need. Security-by-design means analyzing threats and vulnerabilities prior to building the infrastructure. Security-in-depth refers to the anticipated failure of security systems and the assurance of deliberate failsafes. Reflexive evaluation means a continual process that determines threats, vulnerabilities, and risk.

Each of these principles existed prior to the internet and networked systems. The NIST "Framework for Improving Critical Infrastructure Cybersecurity," first released in 2014, also includes each of these principles. However, this security framework includes the dreaded "cyber-" prefix and arrived nearly 30 years after the first networked critical infrastructure systems. The adoption has been underwhelming. A recent GAO report released in February found that of the 16 critical infrastructure sectors, Sector Specific Agencies had developed no metrics to evaluate adherence to or effectiveness of the framework. Meanwhile, each of these sectors evaluate many of the same principles for physical security. These security principles are even declared in the "National Strategy for The Physical Protection of Critical Infrastructures and Key Assets" released in 2003 and have been monitored closely ever since. More importantly, they make sense for any security policy if one considers the first principles.

The inclusion of the "cyber-" prefix adds little more than confusion and a faux technical barrier to the development of policies and procedures. While a subset of critical infrastructure security must consider computer network realities, labeling these considerations as an altogether new domain is ineffective. It draws an artificial rift between the basic security and cyber-security domains. There is no security without cyber-security, and vice versa. By removing the "cyber-" prefix from policy problems, we create an open discussion that allows experts and the broader public to view our "cyber-problems" through well-defined lenses derived from first principles. By dropping the prefix, we may just find new solutions in the traditional method.

SO REMEMBER...
DROP THE "CYBER"

LTJG Brandon Karpf is a Cryptologic Warfare Officer in the Navy. He commissioned in 2015 from the United States Naval Academy with a Bachelor of Science in Systems Engineering where he did research on the attack resilience of SCADA systems. He went on to complete his Master of Science in 2017 from the Massachusetts Institute of Technology where he researched computer networks and cyber policy. LTJG Karpf currently serves at Cryptologic Warfare Group SIX in Fort Meade, Maryland, where he lives with a healthy distrust for all networked systems.