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

The Existential Threat of Cyber: From Hibernation to Cybernation

By Name Withheld by Request

"By failing to prepare, you are preparing to fail." Benjamin Franklin

As residents of planet earth, we are acquainted with the vagaries of Mother Nature—and even if destructive, we know that these are forces we cannot change. Nature and cyberspace, however, are fundamentally different. While natural law sets clear boundaries and dictates events of the land, sea, air and space domains, cyber is man-made, controlled, and adaptable, and, for good or ill, has no natural boundaries. Cyberspace was created to facilitate our communication and connection. Yet, with no clear boundaries, we are all equally advantaged, or can be extraordinarily disadvantaged when cyberspace is used for destructive purpose. Fortunately, unlike in nature, "man-made" means that **people** dictate change in cyberspace and should therefore demand safety and security of their cyber domain.

The residents of this cyber domain, the "users", must now acknowledge that we are in an epic race in cyberspace for competitive advantage in the economic, political and military sectors. The balance of power can change in every one of those categories. Our national security is at high risk because all three of these elements of power can be affected by cyber capabilities, or a single cyber action. This competition and conflict has been going on for three decades, but cyber technology became recognized and actively pursued in the balance of power two decades ago. Now, it is at the forefront.

Our nation has both strengths and weakness in cyberspace. We have great cyber technology because, for all intents and purposes, we created it. Our understanding of this technology, and its applications, are exceptional. We are a technical innovation machine in automation, control system designs and related technical application - the internet of many things. Our advantage is that we were, and are, part of the creation and therefore can dictate change. That said, our ability to accelerate the necessary change is hampered by the unique individuals' innovative spirit that first enabled cyberspace. Unlike our totalitarian adversaries, our nation embraces and educates for individuality, innovation and even competitive challenge. Therefore, we are not of-a-like-mind in recognizing and addressing the threat. Yet, anything that risks national security to this degree becomes an existential threat to our country, our companies, our private lives. It is now personal.

Just as intellectual property is not protected and can be stolen, what we consider to be personal and private cannot be protected, can be stolen, can be misused. We are assuming trust when we pass out our information on the internet; we are not taking personal responsibility for putting it in the cyber environment where there is no enforcement and there are no consequences for somebody stealing it - which in cyber is relativelyeasy to do. If each

© 2018 The Passy Press

innovative individual understands that the key “asset”, the crown jewel of our future, is data, design, and creative application, then intellectual property becomes paramount. All of our information, our intellectual property, can be reached and breached through the internet, cyberspace - stolen, without physically moving anything.

Our government concerns itself with threats to our national security and we do the same with threats to our own privacy, but both are equally vulnerable on the internet and the solutions for both might be the same. So the question becomes how do we defend what needs to be protected when other countries can steal or infringe on patents or intellectual property without fear of consequences? We require enforcement, tough consequences for virtual theft that is equal or greater than that of physical theft. Such consequences underpin protection against cyber theft for individuals, corporations and even nations.

The Commission on Theft of American Intellectual Property estimates that annual costs from the theft of intellectual property, primarily by the Chinese, ranges from $225 to $600 billion, and estimates it will exceed $6 trillion by 2025. The magnitude of those numbers speaks for itself.

Our advantage in innovation is only an advantage if we can protect it. In the corporate and economic environment, the Chinese are active competitors, whereas in the national security environment, they are potential adversaries. They have demonstrated their expertise in using cyber to conduct espionage. But they are not just a country spying on our country; they are stealing corporate assets, knowledge and intellectual property in order to change the dynamic in economic power. If they can get “in” to conduct espionage and steal intellectual property, whether for corporate or national purposes, they then have the capability to deny, to disrupt, and/or change data. Any one of these things can put them well along the way to being able to cause physical destruction as well. Chinese actions in cyberspace facilitate their own economic power while at the same time undermining our economic, military and diplomatic capabilities, thus fundamentally threatening our national future.

It is critical to understand that the Chinese, do not distinguish between economics and national security as we do. Their strategy, which is straight out of Sun Tzu’s *The Art of War* (c. 400-320 B.C.) brings the two together. When they take action, it is to enhance both, whereas we, as a fundamental characteristic of our psyche, laws and culture, keep the two separate from each other.

While perhaps morally or culturally advantaged, democracies are discordant in economic and national action. All totalitarian governments (e.g. China, Russia, Iran and North Korea) fuse together the economic, national security and political sectors, so their response is seamless, fluid and immediate. They have a singularity that gives them an advantage in cyberspace. They can pull all the elements together without separation, whereas we, by definition, separate them all.

The United States, as a nation, creates limits and restrictions for all our government entities, which are at cross-purposes in the cyberspace environment where there are no

© 2018 The Passy Press

domains or physical boundaries of separation. The legal constraints intended to create balance and lanes of responsibility in our government are counterintuitive to cyber, so we have to figure out how to “unconstrain” ourselves to engage effectively in this domain. The U.S. code, for example, applies to every legal jurisdiction in the country, but may form an obstruction to cyber operations unless we can amend or create exceptions for the cyber space. Another area that makes it difficult to conduct cyber operations is the division in Congress for responsibility, which subordinates cyber domain decisions, implications, funding and laws within the traditional committee structure (infrastructure, armed services, banking, etc.) This effectively precludes consistency or efficiency. Our adversaries do not separate these things and bring all that capability together, giving them enormous competitive advantage and decision coherence.

While a healthy suspicion of "big government" is deeply embedded in our national psyche, we cannot allow this bias to blind us to the fact that we are now engaged in an unprecedented kind of warfare, and that our response to this threat must be at a unified federal level rather than piecemeal as it is today. We have agencies and departments that understand cyberspace: offense, defense and exploitation, and these could be empowered to operate more extensively to protect, defend and dissuade.

The massive theft of our intellectual property represents an existential threat to our national security, our economic viability and competiveness, as well as to our expectation of personal privacy for us as citizens. We need a national debate to address this. We might create a standing Congressional Cyber Committee with independent leadership and the authority to override the other standing, select, special or joint committees regarding cyber domain protection and enforcement. Among other considerations, we should also move to establish, formalize and enforce consequences and penalties for virtual theft.

We cannot be complacent waiting for catastrophe to strike. We need to take action now.

© 2018 The Passy Press