The Coming Cyber Pandemic: Part I

While technological advancement has had, undoubtedly, many positive impacts for humanity, it raises complicated questions in the context of increasing global unrest and the changing nature of warfare, national security and international dispute resolution.

By **Niall Brennan, SAP Global Security and Marc Voses, Goldberg Segalla** | July 09, 2020 at 10:00 AM

Introduction

Since the onset of the Digital Revolution in the latter half of the 20th Century, technology has transformed many aspects of the human condition. Our physical borders have become more porous, our exposure to outside influences is greater, our capacity to perform multiple activities has been exponentially enhanced and our interactions are more fluid. In some ways, power and influence have been “democratized” by this phenomenon and the mechanisms to significantly affect large segments of society are available to anyone with a laptop, a wi-fi connection and the technical savvy to manipulate the modern tools of change.

This process will continue to evolve for the foreseeable future. As we adapt how we work, play, live, travel, communicate and interact with our environment, many of the traditional norms of our world order will be altered. The very ease with which people, goods and ideas can, digitally, “circumnavigate the globe” renders our control of the physical world into a much more complicated endeavor.

While technological advancement has had, undoubtedly, many positive impacts for humanity, it raises complicated questions in the context of increasing global unrest and the changing nature of warfare, national security and international dispute resolution. Hostile actors, from lone political activists and financially-motivated criminals to powerful nation states and international criminal and terrorist organizations, now possess the capability to digitally, and anonymously, launch devastating attacks and breaches of critical infrastructure and information systems in the physical world, which equal or supersede the destructive power of the conventional weapons of war.

As such, academics, policymakers and political and military leaders have begun to rethink the traditional definitions and strategies of “global” and “national” security. The dispersal of catastrophic power into a larger pool of potentially malicious, undisciplined hands has altered the battlespace and expanded the “fifth dimension” of global conflict—cyberspace—which defies traditional strategies of border control and national defense. In addition, the fact that cyber conflict occurs in a largely ungoverned virtual space, largely immune to international conventions of war, enhances the risk to civilian populations and collateral victims (e.g. individual citizens, private industry, etc.) and calls for an expanded view of what constitutes defending national security.

This article is divided into two parts. Part I will explore the expanded threat and risk environment created with the unfettered access to destructive power by the weaponization of cyber tools and the anonymity of the modern cyber combatant. Part II will contain an analysis of evolving attack vectors, the expanding list of strategically vulnerable targets, the growing risk to non-military,

civilian populations and conclude with proposing a common-sense, unified approach to developing and deploying controls and regulation in cyberspace.

The Evolution of the “Battlespace” and the Modern Combatant

Core U.S. military doctrine recognizes five domains or “dimensions” of warfare: land, sea, air, space and information. The contours of the first three have defined traditional battlespaces for much of human history. The fourth offers a “bold new frontier” for the future, exemplified by the recent creation of “Spaceforce,” another branch of the United States Military. The fifth dimension of warfare, because it is not a physical space, is harder to define. It has been in significant transformation since the late 1990s from a battlespace previously dominated by human intelligence (HUMINT), signals intelligence (SIGINT) and psychological operations (PSYOPS) to one now dominated by offensive cyber operations. Currently, it represents the most active but least popularly understood domain by which strategic advantage is gained in modern conflicts.

Information warfare has always existed. In a less technological age, it manifested in the form of traditional espionage activities as well as misinformation and “hearts-and-minds” campaigns to gain strategic advantage over an adversary. The Digital Revolution has turbo-charged the development of the fifth dimension, rendering data sets and information systems into strategically important target sets in and of themselves rather than simply the means by which to secure and dominate the historic hallmarks of victory, such as “the high ground,” a capital city or commercial waterways.

Today, combatants gain strategic advantage by mounting offensive cyber operations against adversaries’ data sets and digital processes which transcend the boundaries of the virtual and physical worlds. Though the offensive activity occurs in a virtual environment without the cacophony and spectacle of kinetic military activity, the ultimate impacts occur in the real world in the form of compromised or crippled infrastructures, disrupted commerce, economic loss and human suffering. The cascading effects of these impacts compound the devastation on the same or greater scale as traditional warfare.

Generally, any software (to includes viruses, worms, trojans, etc.) that can be digitally deployed to disrupt an adversary's critical infrastructure, such as national defense systems, communications, public utilities, financial systems, can be considered a weapon of cyber warfare. As such, they are largely indistinguishable from the weapons of cyber criminals, hacktivists or any other malicious cyber actor. In the modern battlespace, standard cyber intelligence collection and social engineering techniques, such as phishing and spear-phishing, are utilized to insert malware on a target system and exploit data and system vulnerabilities, either directly or along a target's supply chain.

Though increasingly sophisticated technology can often facilitate precision placement of specific malware to achieve tailored goals, malware can also easily spread to third parties and other connected entities within a network or intersecting networks and can have unintended consequences. Given the enhanced digital connectivity between government and private commercial interests in the modern economy, this dynamic can represent a significant threat that even exceeds the malicious actor's intent and causes significant collateral damage.

The anonymity that cyber warfare affords its practitioners has also blurred our image of the modern combatant. Increasingly, existing protocols, such as the Hague and Geneva Conventions, which have historically driven our understanding of what constitutes a combatant do not seem to apply. In this orbit, gone is the relevance of uniforms, chains of command, distinctive emblems and, most importantly, conducting operations in "accordance with the laws and customs of war." Even the Tallinn Manual on the International Law Applicable to Cyber Operations (2013), the generally recognized authoritative academic study on how international law applies to cyber conflicts and cyber warfare, struggles with defining the modern cyber combatant and seems to settle for a somewhat imprecise "if it walks like a duck …" argument.

The difficulty lies not just in the anonymity of the celluloid screen but also the deliberate and more effective model for nation states, from a cost, resource and deniability perspective, of "franchising" out offensive cyber operations to tenuously connected or completely unaffiliated proxies, individuals or groups of hackers, who have only the vaguest connection to any

organized chain of command and who receive only basic operational guidance. While history is replete with examples of the failure by organized nation states to minimize collateral damage to non-combatant persons and assets, international law and protocols have created generally accepted standards of conduct.

The blurred connectivity of cyber combatants to a central war planning and analysis element when mounting offensive operations reduces the likelihood that these operations are guided by battle damage assessments and provides little to no accountability. This is a sure-fire recipe for eventual chaos as highly destructive operations are planned and executed in a strategic vacuum.

Niall Brennan is VP for Strategic Partnerships and Engagement with SAP Global Security. He is based in New York City. He has over 29 years of experience in a variety of legal, advisory and investigative roles in both the public and private sectors. Niall retired in 2018 from a 22-year career with the FBI, during which he served in multiple operational and managerial capacities in virtually all investigative and investigative support programs. He has extensive crisis management and international experience and, in his last position, led the FBI office in the American Embassy in Paris, France for over 5 years. Prior to joining SAP, he was a Director in PwC's Cybersecurity & Privacy practice.

Marc Voses is a partner based in Goldberg Segalla's Manhattan office. He serves as the chair of the firm's Cybersecurity and Data Privacy group. Marc has advised clients engaged in business covering a broad spectrum of industries on matters related to cybersecurity and data privacy compliance, and the mitigation of those risks.