

## WHAT HISTORICAL ANALOGIES CAN TELL US ABOUT THE FUTURE OF CYBERSECURITY

By David Sulek and Ned Moran

In their classic study *Thinking in Time: The Uses of History for Decision-Makers*, Richard Neustadt and Ernest May speak to the power and perils of making national decisions through the use of historical analogies. Specifically, they argue for a systematic, critical inquiry to define a problem rather than leaping to a single analogy (e.g., the oft-used Appeasement at Munich) to immediately narrow options and implementation strategies. The systematic use of the appropriate historical analogies can clarify the present situation and afford decision-makers with strategic insights and informed choices. On the other hand, the incorrect application or misinterpretation of an analogy can muddy objectives, narrow options, and create blind spots. A critical element in selecting the right historical analogy(s) is determining the similarities and differences between the present situation and the range of potential historical analogies.

One can debate when cybersecurity first emerged as a national issue, but the Morris Internet Worm of 1988 is a common marker. In the 20 years since this self-replicating program spread across the Internet as a virulent denial of service attack, a significant amount of attention has focused on how best to counter fast-emerging threats and vulnerabilities in cyberspace. In that time, a single historical analogy has dominated US Government thinking: an electronic Pearl Harbor. Even those who do not directly advocate this analogy often employ similar rhetoric, that our cyber systems face the potential of a massive surprise attack that will be debilitating and potentially catastrophic. Beyond the obvious defense implications, this Pearl Harbor is seen as having a greater cascading reach given our society's growing dependence on cyber systems to support every aspect of our political, economic, and social lives.

In the United States and other countries, strategies are shaped by adherence to this analogy. If the analogy proves a correct one, these nations will be better prepared to deal with likely contingencies. However, if the analogy proves incorrect, it may result in missed opportunities, blind spots, and narrow problem definition. Could, for example, a universal focus on such an event and militarizing cyberspace ultimately create a self-fulfilling prophecy, a modern day *Guns of August*? This paper will not argue the Pearl Harbor analogy is a bad one, but rather that: *while an electronic Pearl Harbor is a possibility, it should not be treated as inevitable*. Instead, it will articulate a series of other historical analogies that might inform the future course of cybersecurity. The analogies explored will include but not be limited to:

- **Cyber Katrina:** recently, US cybersecurity expert Paul Kurtz has offered an analogy to Hurricane Katrina, one focused around a catastrophic event occurring (that may or may not be intentional) that overwhelms the ability of government and industry to quick respond and recover.
- **Cyber Sputnik:** this scenario will posit that while the US and other governments are focusing on the security dimensions in a narrow context, we run the risk of another country suddenly developing a leapfrog technology that creates a different type of security dilemma—and an opportunity for the United States to galvanize around a new national vision and investment
- **Cyber Balkanization:** this scenario posits a world where the militarization of cyberspace starts to create a more balkanized structure to the Internet. In this scenario, clusters of Internet connectivity (or even separate Internets) begin to emerge—with what consequence?
- **Cyber Tribes:** the construction of cyber communities of interest fostered through online interaction with people with similar interests and ideologies will further balkanize nation-states and create sub-state level communities with increased organization and power.
- **Cyber Conquistadors:** this scenario posits the United States as a modern day Spanish Empire, a leader in exploring the New World, but one that ultimately sees its power and influence ebb as a new system begins to emerge (e.g., we are now 17<sup>th</sup> globally in broadband access, being quickly passed by economic competitors in Asia and Europe).
- **Cybernization:** this scenario focuses on socio-economic drivers of a post-urban society where the collective power of global users and consumers ultimately drives the future direction of cyberspace.