Lessons from the First Great Cyberwar Era

By A. M. Rutkowski[1]

As we approach the 100th anniversary of the ratification of the international treaty that ended the First Great Cyberwar Era, it seems worth marking the event with a reflection on the steps taken and the extent those actions remain applicable today.

Almost every significant new "cyber" technology has proceeded through the same cycle of behavior by innovators, industry and governments. Excitement, euphoria, and innovation by geeks are followed by industry assimilation and exploitation which gives rise to pervasive public implementations, and then conflict among nations to maintain perceived advantages. Chaos and global cyber conflict then drives international cooperation and accommodations.

The First Great Cyberwar Era

On 22 April 1912, President Taft ratified the first multilateral agreement to which the U.S. became a party – the 1906 Berlin Convention - ending more than a decade of cyber conflict that was implicated as a causal factor in the sinking of the Titanic eight days earlier on 14 April 1912. The sinking and the subsequent investigations so inflamed public opinion that the 1906 Berlin treaty was quickly signed and an additional set of domestic and international actions undertaken by the U.S. government together with other nations in London in 1912 to mitigate further cyber conflict. The London treaty was signed by Taft three weeks before he left office in 1913.

The stroke of Taft's pen approved a global cybersecurity collaborative effort and represented a profound shift in U.S. policies. It was the first acceptance of an international telecommunication treaty by the U.S. - after refusing for nearly 50 years to become a party to any related agreements or instituting any regulation

[1] The author is a leading historian on international telecommunications and law, active in Geneva-based ITU-T international cybersecurity standards activities, a subject matter expert to the White House National Security Telecommunications Advisory Committee, and Distinguished Senior Research Fellow at the Georgia Institute of Technology Nunn School Center for International Strategy Technology and Policy. His own 45 year professional history can be found at www.ngi.org. The views expressed are his own personal perspectives and should not be implied to any group with which he is associated.

of the early wireless cyber environment. Over the succeeding decades, as each new cyber technology emerged, the cyclic pattern has been replicated. Today it is internet technology.

In the late 1890s in a period eerily repeated a hundred years later, major breakthroughs in digital wireless technologies exploded onto the scene, producing new domestic, then global capabilities. As radio waves were unbounded by traditional nation states, wireless internets rapidly emerged worldwide. Any bright entrepreneur or kid with a modicum of knowledge and inventiveness could become part of the emerging global infrastructure. Fortunes were made overnight. However, the problem was that any kid's wireless transmitter in a garage could wreak havoc on a network somewhere else in the world – including those supporting critical business, national security, or emergency needs.

The use of cyber wireless for national security and military purposes had become immediately apparent – especially for ships. The U.S. Navy was an early pioneer, and dominated the U.S. government's development and use of the technology. The first U.S. interagency committee dealing with wireless cyberwar was convened in 1904 and primarily led by the Navy.

As the years progressed during the 1900's, however, chaos emerged. Almost everyone was incented to get on the wireless internet. Commercial business, government, ordinary people, even the equivalent of "script kiddies" and hackers of today – the first radio amateurs – all got "on the net." Enterprises constantly pushed the state-of-the-art; new digital protocols were developed; nations were competing; network architectures and applications were continuously evolving; wireless cyberwar was becoming real.

By 1906, there was a realization of an emerging global problem that no single nation could remedy. Everyone was in this cyber-commons. The world's principal nations gathered in Berlin to develop an international agreement to stave off cyber disaster. They adopted a commonsense, technology-neutral wireless cybersecurity framework that has proven effective ever since.

- **Rule #1 - do no harm**. Every nation agrees that they will take collective global steps that will be imposed domestically on private enterprise to avoid harm to the public infrastructure, services, and communications of other nations.
- **Identity Management**. Network facilities, including those operating them or providing services, will have trusted identities assigned and continually verified by each nation as part of an authorization process that included provider personnel.
- **Effective cybersecurity information exchange**. Nations will share identity and security information in structured formats via a permanent,

trusted Swiss based intergovernmental secretariat, including rapid resolution of assigned identifiers to specific information about the facility or network-service provider.

- **Interoperability**. While respecting the need to innovate, nations will impose obligations to use network protocols, techniques, and operating practices that promote interoperability.
- **Enhance infrastructure resilience and protection**. Every nation will take steps to enhance the resilience of public infrastructure and services and the trust in equipment through technical performance standards, traffic control, and proof of performance.
- **Priority capabilities for emergencies**. Nations will cooperate to provide emergency capabilities during emergencies, especially traffic prioritization.
- **Continuing international cooperation**. Nations will cooperate on cybersecurity for technical, operational, forensics, and enforcement standards and measures to implement Rule #1.

Although the U.S. participated in the 1906 Berlin treaty conference, it would not accept the obligations until 1912 when President Taft ratified the provisions following the sinking of the Titanic. For years, the Washington political scene engaged in incessant wrangling as the wireless infrastructure and cyber security became progressively worse. Private enterprises claimed that technology and innovation would be impeded if the Berlin provisions were implemented, and argued that the infrastructure was overwhelmingly privately owned. Washington lobbyists warned against the dangers of Federal government involvement. There was a general antipathy against foreign nations and intergovernmental organizations. The military community wanted its own freedom of action to keep ahead of the rest of the world. And lastly, there was no consensus on what agency in Washington should act.

The backwash of the Titanic's demise changed everything related to wireless cybersecurity. Essentially all government activity relating to telecommunications in Washington – from the issuing of call sign identifiers and facilities authorizations to the institution of rulemaking and international cooperation - dates to Taft's actions in 1912. The incoming Wilson Administration in 1913 amplified the wireless cybersecurity framework on even a grander scale with combinations of new government R&D and ambitious new initiatives for international cooperation and measures.

The cybersecurity course proved cyclic over the years as each new cyber technology emerged, or administrations and appointees changed, or the U.S. global ambitions advanced or diminished. In general, however, the cycle remained the same. Excitement, euphoria, and innovation by geeks are followed by unfettered industry assimilation and exploitation, which gives rise to pervasive public implementations and then conflict among nations to maintain

perceived advantages. Chaos and global cyber conflict then drives international cooperation and accommodations.

Every new technology generation has gone through the same cycle – whether broadcasting, global telephony, satellite systems, DBS, optical fiber, packet data networks, encryption, or OSI/DARPA overlay internet protocols.

Contemporary Internet Cybersecurity

The focus on internet cybersecurity in the U.S. government appears to have two origins – both about the same time in the mid-70s. When DARPA Director Stephen Lukasik authorized development of the internet protocol technology platform, he secretly asked the National Security Agency to develop a lower layer security infrastructure unknown to the academic-oriented DARPA research community. As the nation's foremost national security scientist, Dr. Lukasik was always the master of the Red Team, and saw the potential threats posed by the internet technology.

The other beginnings of internet cybersecurity revolve round far reaching decisions made within the National Communications System (NCS) in 1976 to undertake a vast program over much of the next two decades across an array of domestic and international bodies that resulted in OSI (Open Systems Interconnection) internet. NCS is a little known but extraordinarily important DOD (now DHS) agency-of-agencies established by President Kennedy to facilitate the resilience, interworking, and emergency use of most national network infrastructures.

In 1976, NCS lead network engineer, Harold Folts, saw the internet platforms being developed in the U.S. and abroad, and called for ambitious coordinated government actions to develop a public internet infrastructure to meet the nation's national security and emergency preparedness needs. In the years that followed, NCS and then DOD and other government agencies together with industry would analyze the potential internet cybersecurity threats and develop combinations of protocols, services, and administrative practices designed to provide a trusted and resilient public infrastructure. Intergovernmental technical bodies like the ITU-T, private international organizations like the ISO and IFIP, and domestic industry technical bodies like ANSI and ECSA were all engaged to pursue these ambitious internet cybersecurity goals.

The enormity of the OSI internet development spilled over to DARPA's R&D community which began leveraging OSI capabilities with simple, security-free versions. DARPA's private internet would have likely remained a historical footnote if it had not been scaled to much broader use thanks to the 1986 Gore Bill's $5 billion funding that included free connectivity and software courtesy of the National Science Foundation. Lukasik's worst Red Team scenarios began

emerging with the unleashing of the infamous Morris Worm in 1988 and the decimation of the now DARPA-NSF internet infrastructure.

In the annals of cybersecurity, the 1988 Morris Worm is also significant because then ITU Secretary-General Richard Butler had convinced most of the world to adopt a new cybersecurity treaty concurrent with legalizing global public internets that same year. The Morris Worm incident occurred three weeks before the treaty body met in Butler's hometown, Melbourne Australia; and courtesy of New York Times reporter John Markoff, descriptions and dissections of the incident appeared daily. As a result, the treaty provisions were amended in an attempt to apply the OSI cybersecurity standards and practices to public internets. The U.S. refused to accept any internet cybersecurity obligations in the 1988 Melbourne Treaty.

During the 1990s, the massive funding and promotion of the DARPA-NSF internet borrowed some of the OSI cybersecurity features and won the marketplace. The single most influential step was Bill Gate's decision to bundle the DARPA internet protocols into Windows 95, subsequently including the Mosaic World Wide Web browser.

Lukasik as DARPA Director Emeritus was able to bring a national focus on critical infrastructure protection in the late 90s, and together with that initiative established the first dedicated program to consider national cybersecurity at Stanford's prestigious Hoover Institute with involvement by nearby Lawrence Livermore Laboratories. He was able to bring together some of the best and the brightest to consider the detriments of the emerging internet infrastructure, and what might be done. His Red Team attacks and Blue Team defenses remain the most comprehensive treatments of internet cybersecurity. The Convention on Cybercrime subsequently adopted in 2001 was one of several emerging steps toward increased cybersecurity.

Over the past decade, other nations have sought repeatedly in different ways to bring about greater cybersecurity and cyber-détente. However, like a hundred years ago, the U.S. response has been mixed and ambivalent, often advancing the same kind of market solution and "no constraint" views advanced during the First Great Cyberwar Era.

The wrong messages began with the U.S. refusal to accept any cybersecurity responsibilities or obligations out of the 1988 Melbourne treaty that legalized public internets. This was followed by facilitating the DARPA internet to trump the more secure OSI internet worldwide, accompanied by avoidance if not refusal to engage in broad multilateral cybersecurity dialogue and cooperation on protection of the infrastructure except in the narrow realm of cybercrime. Unilateral, publicly-vetted consideration of cyberwar capabilities and options layered onto these actions have collectively created a climate of distrust and

increasing potential for cyber-conflict. The resulting instabilities of the cyber infrastructure today are remarkably similar to that of a century ago only on a much larger scale, and with profoundly greater prospective adverse consequences.

An Internet Titanic

Today, most of the world's network infrastructure is still protected to some extent because it is operated by telecommunication providers independently from the implementations of the public internet. Commercial mobile services are also actually more pervasive and growing faster. However, those two worlds are increasingly merging – producing a sense of an internet Titanic moving the network infrastructures increasingly toward major disaster.

Fortunately, the peril seems noticed by governments worldwide and major network operators who recognize the dangers and are moving toward adopting some of the seven necessary steps that became apparent a century ago and stood the test of time in the face of many subsequent new technologies. The new U.S. and UK cybersecurity initiatives are initial tentative steps in the right direction. China, Korea, and Japan are already significantly facilitating global collaboration with effective technical proposals and product mandates – sometimes those developed in the West that have remained unimplemented. However, the U.S. and its political processes and insularity unfortunately tend to resist these kinds of actions even when the dangers are apparent.

The FCC's current major policy making proceeding on a National Broadband Plan is exemplary – where the majority of commenting parties failed to mention cybersecurity. Even those that said something, sought to resist necessary changes. International cooperation was not even treated. Cloud computing was mentioned, but without related security considerations – a stark contrast to the last time the FCC treated cloud computing in the 1980s. The dark cybersecurity clouds on the network horizon portend of the perfect cyberstorm. As of July 2009, the latest cyber Shock and Awe statistics Spain's Panda Networks was detecting 37 thousand new viruses, worms, Trojans, and other security threats per day, and reached a total of 30 million different varieties. Other analysis has demonstrated that the majority of these threats emerge from U.S. based infrastructure because of the centricity of the nation in the legacy global internet architecture.

For the First Great Cyberwar Era, it took a dramatic incident like the sinking of the Titanic to bring about major change in U.S. policies. Will that be the case again today, and what will be the requisite level of Shock and Awe to obtain substantial U.S. action and cooperation? It is long past due to institute the seven proven components of a global cybersecurity framework.