The Cold War and Cybersecurity

Klaas Voss /
Hague University

The five "Domains of Warfare" are a core concept of modern military science. They delineate a simple principle: Technological prowess can be parlayed into military superiority when it is harnessed to control new fields ("domains") of military activity. Land, sea, air, space – each of these fields has seen its own age of military pioneering, dominated by submarines and chariots, chronometers and GPS satellites. The Cold War is of course rightly associated with the US-Soviet rivalry in space, which became synonymous with the race for the best delivery systems for nuclear weapons and the most high-performance intelligence and navigation satellites. There was another military realm, however, which was explored and exploited especially in the Cold War's final decade. In 1995 a US Air Force general christened it the "Fifth Dimension of Warfare", i.e. the virtual world of information. Even earlier, in the 1980s, a different term became the standard, that of cybernetic space or "cyberspace".

The trans-disciplinary science of cybernetics, which sought to make all fields of society open to planning, control and interconnection, was no less a project of the Cold War than was game theory, the mathematical operating system for nuclear war. Also and particularly remarkable is the societal significance of cybernetics and early information technology in

the Soviet Union, which Slava Gerovitch has traced in his writings. While the Soviet administrative apparatus still dreamed of the perfect "cyber bureaucracy," by 1969 the US Advanced Research Project Agency had already developed the Arpanet, the technical prototype for what would become the Internet. Although it is a myth that this project was exclusively military in nature, seeking to preserve nationwide communications in case of a nuclear strike, the history of the Internet is nonetheless inseparable from the Cold War and the threat of nuclear weapons. In 1960 the RAND Corporation produced a study on the use of digital telecommunications networks to assist the rebuilding process following a nuclear strike. Some passages are too bizarre to paraphrase:

"The cloud-of doom attitude that nuclear war spells the end of the earth is slowly lifting from the minds of many. Better quantitative estimates of post-attack destruction together with a less emotional discussion may mark the end of the 'what the hell – what's the use' era. [...] If war does not mean the end of the earth in a black and white manner, then it follows that we should do those things that make the shade of grey as light as possible: to plan now to minimize potential destruction and to do all those things necessary to permit the survivors of the holocaust to shuck their ashes and reconstruct the economy swiftly." (Source)

Just how much the subsequent Internet would have helped to "shuck the ashes" of a nuclear war must remain a matter of speculation. Yet as early as the Carter and Reagan administrations, the NSA and US military were issuing strategy papers on the security of digital communications pathways and data sets. This was the birth of cybersecurity, which in the

following years would become a new frontier of national security and has remained one ever since.

In a new project, the National Security Archive at George Washington University in Washington, DC, is using the Freedom of Information Act (FOIA) to shed light on this barely-explored area of US security policy and makes previously classified documents regarding all sorts of "cyber issues" from both state and private sources available to researchers and the interested public. The Cyber Vault project currently comprises a full text database of 388 documents from between 1964 and 2016. This may seem modest at first glance, but anyone acquainted with the National Security Archive's previous work might expect this figure to rise. The archive includes more than 45 fully digitized collections with a total of more than 104,000 documents, many of them stemming from the intelligence, military or presidential domains and with (originally) high security classifications. For many historians of the Cold War investigating sensitive fields of US foreign and security policy, working with this institution's collections is somehow a rite of passage. Despite the time-consuming process of submitting FOIA applications, then, we can hope that the Cyber Vault project's collections keep growing rapidly. Following an initial perusal of the Cyber Vault project's database several seeks ago, the collection has already grown by 25%.

Jeffrey T. Richelson is a Senior Fellow at the National Security Archive and Director of the Cyber Vault project. Many of his publications deal with the interfaces of military and security policy, technology and science. In an email, Richelson states the objective of the new project:

"It was apparent that while there was a vast literature on cyber issues, references to documents, and occasional postings of documents, there was no collection of such documents that came close to being comprehensive. It seemed clear that such a collection would be interesting and useful to both those researching contemporary cyber activities (whether cybersecurity, cyber espionage, or cyber war) as well as looking back into earlier years. The objective is to establish a major repository for such documents that would allow researchers to find both individual documents relevant to their work but also sets of documents that would facilitate their research."

Although Richelson also notes that the relationship between the Cold War and cybersecurity issues is not the focus of the project, this in no way diminishes the usefulness of the published documents for research in this direction. For example, one RAND paper from 1967 warns against foreign (especially Soviet) attacks on US military computer networks: “Computer systems are now widely used in military and defense installations and deliberate attempts to penetrate [them] must be anticipated.” It might have been an innovative idea in 1967 that computer systems must be protected against spying. The vulnerabilities described in the RAND paper, on the other hand, seem quaint from today’s perspective. Whereas IT experts now fear rootkits, DoS attacks and botnets, the engineers of 1967 warned against security lapses stemming from the exchange of monitors (then an integral system component) or eavesdropping on electromagnetic waves from processors or cables. Terms “virus” and “Trojan” were not yet commonplace. Instead, the word today meaning software problems was

used: “bug.” This “bug” inserted by spies was “some computer equivalent of the famous transmitter in a Martini olive.” Yet the IT engineers in 1967 also recognized that the greatest security risks were found among users (In this respect at least, IT experts have changed little). The possible monitoring of electromagnetic emissions from cables and processors by intelligence services caused great consternation into the 1970s as a declassified report by the US Defense Science Board Task Force for Computer Security makes clear. The method may be reminiscent of Morse code in the telegraph age, yet we should refrain from treating these specialists’ warnings with premature condescension. To this day, a large segment of network traffic is still conducted through copper (i.e. not fiberglass) cables, meaning that it remains vulnerable (at least theoretically) to attacks of this kind.

During the 1970s and 80s the burgeoning field of cybersecurity increasingly became an issue for national security, concerning intelligence services, the Pentagon and the White House. “Cryptolog,” the NSA newsletter, devoted several issues to the discussion of new security concepts. One issue made available by the National Security Archive from the year 1979 mentions (as fields for future research) a whole series of these key elements of modern IT security – practically in passing. Perhaps the most engrossing published document from that time of the Cold War is, however, President Ronald Reagan’s National Security Decision Directive #145 of 17 December 1984. Here, Reagan explicitly declared the protection of “automated information systems” to be an executive matter. This has since become a “vital element of the operational effectiveness of the national security activities of the

government and of military combat readiness." The World Wide Web – for most people a synonym for the Internet – did not even exist at that point, yet the IT integration of military and government institutions had already rendered the growing realm of cyberspace a new frontier of national security. By then, Reagan's concerns were no longer directed solely at the Soviet Union and other foreign countries. The future threats to IT security, as NSDD 145 states, would also emanate just as much from terrorists and criminals. It was a perceptive conclusion.

Dr. Klaas Voß is a lecturer for "Safety and Security Management Studies" at the Hague University of Applied Sciences.

Recommended Citation:
Klaas Voss, The Cold War and Cybersecurity, 08/30/2016, http://www.berlinerkolleg.com/en/blog/cold-war-and-cybersecurity (please add the date of the last call to this page in brackets).