2015

Pelikan's Antidisambiguation--World War III, or Simply War, ver. 3.0--A Soft Rollout?

Michael P. Pelikan
Penn State, mpp10@psu.edu

Pelikan's Antidisambiguation — World War III, or Simply War, ver. 3.0 - A Soft Rollout?

Column Editor: **Michael P. Pelikan** (Penn State) <mpp10@psu.edu>

They called it the Great War, at least until the outbreak of the Second World War, after which it came to be called the First World War. Its causes were complex, multi-threaded, and spread out over time. Frequently-cited were the partially overlapping, sometimes colliding web of treaties and alliances that led to disaster, creating apparently unstoppable chains of cascading events. Once begun, the only "way out" was "through."

The result was "…a clash of 20th-century technology and 19th-century tactics, with the inevitably large ensuing casualties," a characterization found in the surprisingly good (and ever-improving) Wikipedia main article, "World War I." The technology had advanced faster than the tactics, or for that matter, the ability to cope with the casualties. Among the new technologies on the battlefield were the telephone, wireless communications, armored cars, tanks, and combat aircraft. There were new and newly lethal weapons deployed as well, heavy artillery, rapid-repeating guns, and most despicable, chemical weapons.

The aftermath of the First World War included a completely redrawn map, and an international community so fed-up with Germany that it was deemed a suitable solution in the Treaty of Versailles to compel upon that state near-total disarmament, (a pact characterized in Wikipedia as "neither lenient enough to appease Germany, nor harsh enough to prevent it from becoming the dominant continental power again"). The unintended consequences this led to were founded in the bitter resentment that bred among the people of that country, offering fertile ground for the twisted diagnoses and remedies offered up a couple of decades later by **Hitler**.

The Second World War brought even more radical developments in the technologies to support and advance warfare: aircraft (long-range strategic bombing, jets, high explosives, nuclear weapons), naval (submarines, battleships, aircraft carriers), and of course, cryptography (Enigma, for one) and the information technology to counter it (Ultra, Colossus, ENIAC), leading to advances in all other technologies.

Out of the Second World War we came into the Cold War, carrying us, depending upon the dates we apply, from the late 1940s into the early 1990s. By the end of that period, we had gone to the Moon, heard a young **Bill Gates's** vision for "a computer on every desk and in every home," and seen **Tim Berners Lee** propose an information management system to the **European Organization for Nuclear Research** (better known as **CERN**) based upon links embedded in readable text. "Imagine," wrote **Berners Lee**, "…the references in this document all being associated with the network address of the thing to which they referred, so that while reading this document you could skip to them with a click of the mouse." (See Wikipedia's main article "History of the World Wide Web.")

Through the benefits of hindsight, it's possible to see clear threads running from the aftermath of the First World War directly into the Second World War. Similarly, it's possible to find clear traces running from the aftermath of the Second World War into the Cold War and its political and technological "areas of concentration." It wouldn't be surprising, therefore, to

find that a kind of "advance hindsight" applied to the trends of the last twenty years might offer clues to the state of affairs prevailing in the world today, and leading into the future.

The realm of activity we arrive at is that encompassed in the term "Cyberwarfare." What this term really means, what it captures and includes, are matters both of common recognition by average folks, and yet widespread ignorance as well. Using readily accessible information resources, it is possible to become reasonably well-introduced to the topic. I offer no apology for referring you, once again, to the ever-surprising, ever-improving resources available in Wikipedia. If you haven't done so, and if you're at all interested, please take a look at Wikipedia's main article on Cyberwarfare, at *https://en.wikipedia.org/wiki/Cyberwarfare.*

There are a few aspects of this realm that bear emphasis. The first key idea I'd wish to highlight is that the activities encompassed by the term "Cyberwarfare" are activities undertaken by nation-states. In the present time, there are organized activities underway that do not originate simply from adolescent hackers or organized crime groups, and that are not simply the inevitable consequence of inept security or data gathering practices by big corporations. The Wikipedia article I've cited above begins with a definition of "Cyberwarfare" from **Richard A. Clarke** as, "…actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."

The second point to take onboard is that these activities bear the marks of strategic planning, well beyond simple identity theft or trying to grab credit card numbers to exploit. For example, it is a proven pursuit of nation-state-sponsored Cyberwarfare to establish layers of hidden infrastructure, paving the way for its own further use. These efforts are most successful when undiscovered, and, of course,

we can't prove what we haven't discovered yet. But what has been uncovered, and documented, are large-scale, organized efforts to compromise large, well-established networked resources, to put in place identities with elevated privileges on those networked resources, and to facilitate follow-on or subsequent actions. This is the Cyberwarfare equivalent of establishing Sleeper Cells, quietly building and placing assets to be activated and used at a later time. This is the specific reason behind some of the large-scale compromises of systems that are uncovered and publicized after the fact.

What ultimate strategic aims lie at the heart of such activities are, for this mere mortal, a matter of conjecture, but the potentialities inherent in the presence of as-yet undetected, in-place Cyberwarfare assets are terrible to consider, and important to recognize. As everything we do in normal daily activities moves further and deeper onto networked, "cloud-like" resources, the potential points of impact increase.

Our routine activities, our use of social media, of networked storage and file-sharing resources, of network-based entertainment and news and information resources, of e-commerce in all its forms, are like trails through a jungle: necessary to get through the dense undergrowth but difficult to hide, and shockingly easy to observe quietly from a distance.

As they've said in the face of previous threats, "You can't stop living." And neither can the companies and large-scale organizations with whom we deal every day. Airlines, utilities, banks, hospitals, educational institutions, government entities at the local, state, and national level, all are undergoing continual, active investigation and probing by state-sponsored entities who do not have our best interests among their top priorities.

Our extensive use of networked resources makes those resources a strategic target, even though the larger strategic objectives of those state-run entities pre-exist. What we must do is become more than passingly-familiar with the kinds of tactics and methods in use today. We

can learn about these through openly available resources. If you're in a position of supervision or ownership of networked resources, it's probably time to become well-acquainted with the potentialities, pitfalls, and opportunities for action available to you. Learn what you can. Read what you come across. Observe the actions taken by companies and organizations in response to such state-sponsored activities. Don't skip past those stories assuming it's "just another hacker" or "just another company caught unprepared."

It's important to encounter and get through some of the shock of discovery now, under circumstances under our control, rather than after it arrives at our virtual doorstep amidst a real-world incident.

If you're at all interested, take a look at the Wikipedia article I've cited above. Maybe look through some of the references that article contains, or jump to related articles and resources. Along with the inherent potential exposures and vulnerabilities that have emerged, we're also in a time of prodigious blossoming of positive, credible resources, freely and readily available to any who are curious, to help us come to know the world in which we live.

The dates associated with wars frequently mark specific turning points in complex, evolving series of events already underway. Armed conflict seems most often to start with the opposing sides already identified, known to each other and to the rest of the world. The outbreak of an armed phase of belligerence seems most often to be an extension to existing areas of disagreement and concerted action taking a more serious turn. All these observations contribute to a sense that opposing forces, state-run and acting on those states' behalf, have already taken the field and are in action.

What, specifically, the present day leads to is, of course, as yet unknown. Once whatever that is has become known, it doesn't seem too great a stretch to suggest that, looking back, we'll see its roots were present, visible, and even identifiable, in the present day. 🐦