Digital Age Superiority …or the Digital Dark Age Collapse

by William B. Scott

> ***Cyber may be one of the most consequential national security challenges in a generation, and it will not grow easier with time. Our adversaries now believe that the reward for attacking the United States in cyberspace outweighs the risk.***
>
> ***— Senator John McCain[1]***

The Digital Age, whether you like it or not, is not upon us—it is now. The industrial age began over 200 years ago, and the large-scale factories of old, focused on mass-production of replaceable parts, have given way to decentralized, customizable, online orders. As government officials, policymakers, analysts, and computer programmers attempt to address deterrence, guard against possible incursions from adversarial belligerents, and compile doomsday scenarios for national leaders, they often overlook the inherent flaw in mastering the current digital architecture: It is not run by any government. Multinational corporations hold the keys to the digital kingdom and may lead the global community to a digital age collapse.

Adopting New Technologies

Imagine life 3,000 years ago: an industrious civilization just began smelting iron providing a great technological advantage over the other nations using bronze. Wrought iron, although not stronger than bronze, bends and chips under stress rather than shattering.[2] Naturally it would get incorporated in armor and weaponry which gives the military an advantage. It can also be sharpened after combat rather than melted and remolded. The metal's ready abundance gives an economic advantage over the relatively rare tin necessary in the production of bronze. In this situation, iron would become the hallmark of the civilization. It would be unthinkable to allow such an impressive technological advancement to be managed by an iron guild that did not play nicely with the blacksmiths, weapon smiths, and armorers of bronze that could fully utilize the advantage of iron.[3] Since the Hittites were

Major William B. Scott is an intelligence analyst and foreign area officer for the United States Army. Currently working at the Pentagon in HQDA G-2, he holds a B.S. from New Mexico State University and a M.A. from Vanderbilt University.

the first to smelt iron ore, it would be marked as the most significant factor to the expansion of the empire…except it is not! Although the Hittites were the first to smelt iron, it was not integrated into the military that expanded the kingdom with bronze weaponry. When iron was finally incorporated fully in combat, it was used by various factions, causing the Late Bronze Age Collapse. It was the most violent, sudden, and culturally-disruptive disaster in ancient history when many cities were fully destroyed, and regional empires were devastated into villages and tiny city-states.

Despite the fact that over half the world uses the internet, very few outside of the information-technology community actually understand the general architecture, which is dangerous…

Historically, there is always a hesitance for established powers to incorporate new technology. The Hittites at the time had the strongest military in the region—why fix it? Although in hindsight, it is incredibly obvious for an empire to convert to iron, contemporary experts would argue against converting to iron because bronze is less brittle, has a lower casting temperature, resists corrosion and rust, and is stronger. However, had the Hittites quickly capitalized on their ability to smelt iron, their advancements would have surpassed the Roman Empire. Failing to adapt to a different metal led to a Dark Age noted for the destruction of civilization in the region for the following 300 years.

Iron brought significant changes to daily life in the societies that mastered it, from assured victory in battles to larger crop yields in farm fields. Exploiting tougher soils allowed the Iron Age denizen to experiment with different crop varieties and techniques. Iron carts and horse bridles allowed transport of heavier objects and cargo, increasing distance over land trade routes.

Digital communication is having the same world-changing effect that smelting iron had 3,000 years ago. Words such as social media, cell phones, cyberspace, email, digital currency, and video teleconferencing were non-existent or relatively unheard 30 years ago. Furthermore, cyberwarfare, cybersurveillance, telecommunication, ecommerce, and identity theft have changed lives socio-economically and added complexity to ensuring security, accountability, and identification. The digital age has changed our lives, and it continues to shape our world in sometimes unforeseeable ways.

The United States initiated the Digital Age when the United States Department of Defense funded universities to develop a method of packet switching in the 1950s, establishing Advanced Research Projects Agency Network (ARPANET) in 1969, the forefather of the World Wide Web. Commercial Internet Service Providers (ISPs) emerged in the late 1980s, and by 1990 ARPANET was decommissioned. At that time, approximately 1 percent of technologically-stored information in the world was in a digital format. As online commercial industry prospered, more information became stored in an interconnected network known as the internet or cyberspace. By 2014, more than 99 percent of stored information resided in digital rather than analog format. As tablet computers and smartphones began exceeding personal computers for access to the internet, half of the world became connected to cyberspace by 2016.

Understanding the Internet

Despite the fact that over half the world uses the internet, very few outside of the information-technology community actually understand the general architecture, which is dangerous, as it has allowed the industry to grow without oversight to its effect on national security.

In fact, often nations are more concerned as to what information is openly accessible inside the internet versus the construction and architecture of cyberspace. To avoid a Digital Age Collapse, it becomes imperative for nations to secure digital interests akin to physical ones. A basic understanding of Internet Protocol (IP) fundamentals, however, is essential to understanding the limitations and improving the digital domain. An investigation into the relationship between different forms of software will help define how cyberspace is shaped in this current Digital Age.

First, what is exactly meant by bandwidth? Most people have a general idea that the more bandwidth one has, the faster one can download a webpage, so, often, bandwidth is used interchangeably with data speed; however, it is more than that. Bandwidth relates to the physical means to attain internet connectivity. In short, without bandwidth, there is no connectivity, hence, no cyberspace. Bandwidth can be increased easily one of two ways: increase the efficiency of the connection or add more connections between the receiver and transmitter. The simplest way to understand bandwidth is to think of it as a road network. The more roads in an area relative to the vehicles equates to less congestion. The better quality of the roads (i.e., dirt vs. paved multilane) means the faster the vehicle can travel. As of 2015, three countries maintained 50 percent of the bandwidth of the world,[4] which is important because it allows for multiple avenues that packets of information can travel from one terminal to another, but what exactly is a packet, and why does it matter?

The packet is the crux of packet-switching technology, which allows cyberspace to exist. A packet is a pre-established set of codes that contains control information that provides instructions for delivering data and the data itself. Although there are different possible versions of packet protocol, the majority of cyberspace uses version four of the Internet Protocol (IPv4)[5] developed back in 1981, which includes formatting, error detection codes, sequencing information, and network addresses. Packets may also contain sensitive raw data such as financial transactions and passwords. What it does not included is encryption, guarantee delivery, dynamic addressing to keep up with the growth of the Internet, and tracking of the actual packet. IPv6, the successor to IPv4, has addressed many of these issues, but due to the enormous established infrastructure of IPv4 routers and ISPs, IPv6 remains mostly unimplemented despite many planned initiatives to transition. Without mandated governmental change, the cyberspace infrastructure remains in IPv4, and packet design limitations and capabilities determine the basic limitations and capabilities of the interconnected network.

A basic understanding of Internet Protocol (IP) fundamentals... is essential to understanding the limitations and improving the digital domain.

Information Security

Computers, tablets, and mobile phones allow access to the enormous amount digital information on the internet. It is important to note that no two connections are the same: aside from the multitude of computers, tablets, and mobile phones one can use to access the internet, there are also peripheral devices such as printers, speakers, external keyboards, monitors, etc. Each is managed by its own firmware, permanent software in read-only memory (ROM). In addition to the firmware of peripherals, at any given moment there can be dozens of other software programs running on a device that access the internet, each with its own vulnerabilities and weaknesses. There are a surprising number of backdoors and flaws

developed in the industry, and no one is held liable for producing a substandard product, such as poorly-programmed software that compromises security of sensitive information. Instead. the industry is allowed to keep quiet, and the more responsible software companies occasionally push security updates over the internet, in some case mandating and forcing additional updates, which require the users to be connected online.

...although there is abundant means to generate and store data, paradoxically there is not a practical means to preserve the data forever.

In short, the industry is allowed to police itself, and industry's final objective is to earn money, rather than look out for the best interest of the nation. Very few governments actually manage the software to their own systems. This may be because cyberwarfare is in its infancy. To date, only one country has used cyberwarfare in full multi-spectrum combat,[6] but each day the pool of malicious attacks inside cyberspace continues to grow. Threats range from espionage to immediate damage or disruption to vital military and civil services such as electricity, finance, and communication. Often these threats come in form of viruses, worms, Trojans, spyware, and ransomware. Despite the growing complexity and focus on cyber defense placed on servers and workstations, governments and corporations continually find the backbone to their network system compromised. Policymakers often ask an analyst how one nation can acquire digital dominance in cyberspace. The statement is too vague because how does one judge digital dominance? An analyst may answer the question by indicating that it is the bandwidth growth and capacity, the amount and type of hardware existing on the network, and the quantity and expertise of the programmers residing in the country or focus on how the nation can effectively leverage a mixture of these elements to effectively target another digital infrastructure in cyberspace. It is, however, a trick question. Although nations have vested interests inside the internet and employ programmers to secure and support critical assets in cyberspace, the reality is the majority of control to keep networks secure is in the hands of multinational corporations, and with few exceptions, nations and criminal organizations have access to their products.

Data Degradation and Loss – A Digital Dark Age Collapse

Unfortunately, there is another sinister problem afoot. In 1997, Terry Kuny postulated during a conference at the International Federation of Library Associations and Institutions about a Dark Age of recorded history due to digital technology storing information. A Digital Dark Age, however, is more than just theory, it has already begun. Almost all information currently stored is in a digital format, and although there is abundant means to generate and store data, paradoxically there is not a practical means to preserve the data forever. The fact is that the means to read the digital information itself degrades, corrupts, and becomes obsolete over time. In the last few decades, digital data has changed considerably. The means to read data stored on older devices, such as punch cards, floppy disks, and zip drives, have all but vanished, much less the programs to run them. Corporations constantly "improving" technology sometimes result in file incompatibility, so proprietary programs become incompatible with earlier formats.

Although vital information can be backed up, there is no guarantee that future generations will be able to access important files such as scientific research, government documents, and contemporary recordings of historical events. As

documents transfer to digital formats, often the original copies are not preserved. It is not difficult to imagine a future where knowledge is lost due to natural disaster or worse, cyberwarfare combined with conventional combat. The knowledge that has been passed and grown from generation to generation will simply disappear. Our children, grandchildren, and great grandchildren will marvel at the achievements of their forefathers as they try to unravel the mysteries from the few isolated networks and individual computers. The greater part of the information in the World Wide Web will be gone; details of a century of unprecedented accomplishments will be lost; scientific knowledge will have to be rediscovered and technological advancements reinvented. – It will be a Digital Dark Age Collapse.

Life After the Digital Dark Age Collapse

Life after the Digital Dark Age Collapse will still be digital. Dependence on digital mediums will not cause devastation to civilizations; society will collapse because like the innovation to smelt iron, leaders failed to envision the importance of the new technology before it was too late. Our descendants will rebuild interconnected networks from the ground up. Governments will regulate how the connectivity is built and keep certain elements of the architecture a national secret. They will be smaller and more flexible, and the militaries and emergency forces will be able to commandeer bandwidth easily during a national emergency. The doctrine of the basic soldier will include hacking enemy networks; there will be specializations as the architecture of each enemy network will be significantly different from another. Friendly nations will still have access through identification tokens for the purpose of commerce and communication. Operating systems and processors will be regulated by a commission, ministry, or secretariat, and although the graphical user interface will seem identical inside a nation, the mechanics underneath will contrast greatly in capability between the official government operating system and what is available on the open market. Companies that do not follow the tightly controlled regulations will be fined, shut down, or the senior executives will face incarceration. Digital capability in cyberspace will become a munition, and to prevent the Digital Dark Age and a Dark Age Collapse, probably should be treated as such now.

Indulge me, in a silly scenario: You are the leader of the industrious civilization during the Bronze Age. Citizens of your empire have developed a technique to smelt iron, which would give your forces a military advantage over the enemy, a crop-yield advantage over neighbors, and an economic advantage over trade partners. If you destroy the iron-clad dominance of the guild, you can avert the Bronze Age Collapse and the Dark Age that followed by incorporating and regulating iron in every aspect of trade, agriculture, and the military. Smelting iron would quickly be adopted by other societies, but the quickest source of iron would be your nation's farm tools—tools made from lower grade steel than what had been developed for the military. Your empire would dramatically grow in strength to be the envy of history. Now, imagine that you are leader of an industrious civilization today at the cusp of Digital Dark Age, what do you do? ***IAJ***

NOTES

1 John McCain, "Cyber Strategy and Policy," hearing to receive testimony, Committee on Armed Services, United States Senate, March 2, 2017.

2 Steel is in fact stronger than bronze, which can be made by adding as little as 2 percent carbon to iron. There is much debate as to whether early wrought iron or crude steel changed the dynamics in the late Bronze Age, as the early crude furnace process allowed smoke (carbon) to enter iron. For the sake of this argument, I have assumed that early iron at the end of the Bronze Age had some carbon but not enough to refine it to steel as conventionally known.

3 This is admittedly speculation. It is currently unknown whether the Hittite civilization was organized under the guild system or not, but it is plausible.

4 The three countries are the United States, China, and Japan. Martin Hilbert, "The Bad News is that the Digital Access Divide Is Here to Stay: Domestically Installed Bandwidths Among 172 Countries for 1986–2014," *Telecommunications Policy*, Vol. 40, No. 6, June 1, 2016, <http://escholarship.org/uc/item/2jp4w5rq>, accessed on April 4, 2017.

5 IPv4 is in fact the first version of Internet Protocol, and IPv6 is the second version.

6 Russia and/or Russian supporters preformed a denial of service operation against many Georgia websites in South Ossetia weeks prior to actual ground movement during the Russo-Georgian War in 2008.