AIR WAR COLLEGE

AIR UNIVERSITY

CYBER CAPABILITIES FOR GLOBAL STRIKE IN 2035

by

Dean A. Clothier, Col, USAF

A Paper Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

15 February 2012

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Colonel Dean Clothier is a U.S. Air Force aviator and cyberspace defense officer assigned to the Air War College, Air University, Maxwell AFB, AL. He holds a Bachelor of Science degree in Computer Science & Engineering from the University of Texas at Arlington, a Master of Business Administration from St. Mary's University of Texas, and a Master of Arts in military operational art and science from the Air Command and Staff College. He is a master navigator (electronic warfare officer) with over 1,400 flying hours in the EC-130H Compass Call and T-43, and recently achieved his master cyberspace badge. He is a graduate of the USAF Weapons School, has served at both the MAJCOM and the Air Staff, and is a graduated squadron commander. He flew combat missions in Iraq and served as the JFC's Command EWO in Afghanistan.

Abstract

This paper examines global strike, a core Air Force capacity to quickly and precisely attack any target anywhere, anytime, from a cyber perspective. Properly used, cyberspace capabilities can significantly enhance Air Force (AF) capabilities to provide the nation the capacity to influence the strategic behavior of existing and potential adversaries.

This paper argues that the AF must improve both the quantity and quality of its cyberspace operations force, by treating cyber warfare capabilities in the same manner as it treats its other weapon systems. It argues that despite preconceptions of future automation capabilities, that cyberspace will be a highly dynamic and fluid environment characterized by interactions with a thinking adversary. As such, while automation is required, cyber warfare will be much more manpower intensive than is currently understood, and will require a force that is very highly trained. The rapid evolution of this man-made domain will also demand a robust developmental science and research investment in constantly keeping cyber warfare capabilities in pace with the technologies of the environment.

This paper reaches these conclusions by first providing a glimpse into the world of cyberspace in 2035. The paper then assesses how cyber warfare mechanisms could disrupt, disable, or destroy potential adversary targets. It describes how these capabilities might work in two alternate scenarios, and then describes the steps the AF needs to take in the future to be confident in its ability to "fly, fight, and win…in cyberspace."

Table of Contents

Introduction

It is a simple question, "By the year 2035, how should the USAF use cyber warfare capabilities to perform *global strike* missions?" The establishment of 24th Air Force as the Air Force Cyberspace Command (AFCYBER) clearly shows USAF leadership embracing the need to strengthen its cyberspace warfare capabilities. This portends a growing role for cyber in many Air Force functions. This paper argues global strike is one of the AF's core capacities, and planning to use cyber to generate future global strike capabilities is essential as we look toward the 2035 time frame.[1]

This paper begins by examining the likely nature of cyberspace in 2035. It then explores the implications of cyberspace changes on expected global strike targets, and how cyber may affect those targets. It then examines the composition and characteristics of future cyber weapon systems that could perform global strike. Finally, the paper argues the consequences of failing to field these cyber warfare capabilities will likely to lead to sharp reductions in effectiveness, particularly in areas of anti-access and area denial (A2/AD) threats that may limit traditional global strike capabilities and methods.

[1] The time horizon for the Blue Horizons program is 2035. See: Memorandum from General Norton Schwartz, AF/CC, "Invitation to Participate in the Blue Horizons Program for Academic Year 2012," 19 May 2011.

Cyberspace in 2035

Why think about the cyberspace environment in 2035? Because unlike the air and space domains, cyberspace is itself "constructed" using high technology components. In the 20 years since the birth of the Internet, cyberspace has undergone radical quantitative and qualitative change. The emergence of media distribution, consumer channels, social media hubs, and vast public information utilities are examples of profound qualitative changes to the Internet that have occurred. Making cyber warfare predictions based on the unstated assumption that a future cyberspace is merely bigger and faster will lead to fundamentally erroneous conclusions. Cyberspace in the future will not merely be better, it will be fundamentally different.[1]

The current exponential growth curves for cyberspace mirror the early growth curves for aviation. Cyberspace has shown an incredible rate of technological change from December 1990, when Tim Berners-Lee first brought the world-wide web to life, through the present.[2] Aviation technology growth from the Wright brothers' famous flight on December 17, 1903, through the next 20 years followed a similar path. Both paths consisted of a few years of rapid experimentation, then early commercial adoption, followed by a surge of new technologies in response to emerging applications and markets. Looking forward to 2035 cyberspace capabilities is comparable to the change that occurred from the post-WWI bi-planes of 1924 to the B-47 Stratojet of 1947. The impending change in cyber will be qualitatively and quantitatively massive.[3]

Future Cyber Devices

The future cyber domain will penetrate nearly all elements of nations, communities, and individuals, becoming a critical aspect of everyday life.[4] The spread and evolution of cell phones and personal computing devices will expand the cyber domain to nearly every nation on Earth.[5] Virtually all communication, information, and entertainment streams will be digitized and ride on a heterogeneous mesh of IP-centric transport systems, which will be a direct outgrowth of today's Internet.[6] Understanding the key characteristics of the Internet requires examination of the networks themselves and devices that enable user access.[7] ◘

The diversity and proliferation of end-user devices will see continued growth driven by technology, economics, and human factors. Computer technologies will continue exponential performance growth resulting in specialized product technology lines that together enable an ever richer and more capable ecosystem of end-user devices. Despite some predictions of the impending death of Moore's law,[8] many experts see it continuing for at least 15 more years.[9,10] Corollary gains in memory, storage, graphics, and bandwidth should also be expected, as they have roughly tracked with Moore's law.[11,12] These trends often lead to predictions that singularly focus on more powerful desktop machines, or smaller laptops with increased capabilities, or ever cheaper PCs.[13] What is commonly overlooked is that these predictions hold true independent of one another, and look to do so for the foreseeable future.

Commercial economic forces are the primary drivers of cyber technology. One mantra among cyber entrepreneurs is "If you can't get it to scale, it doesn't matter."[14] The effects of economic trends on smart cell phone proliferation, the global diffusion of Internet connectivity, and the expanding number of economically viable device product classes are resulting in cell phones driving Internet expansion for much of the developing world's population. Compared with laptop computers, the longer battery life of cell phones fits well with the partial electrification of poorer states. The result is that, "In 2020 … the mobile phone—now with significant computing power—[will be] the primary Internet connection and the only one for a majority of the people across the world."[15] Further, the character of cyberspace will also be greatly affected by the growing capabilities of cell phones.[16]

Steadily decreasing device costs, coupled with continuing increases in the value of Internet access for individuals, will continue to drive Internet expansion. The economic "network effect" is the driver. Loosely stated, the "network effect" occurs where the more people using a given network, the greater the value the network has to each individual.[17,18] Specific Internet services or functions, however, may gain only "local" effects because individuals only value interacting with a relatively small social subset of users.[19] One example is the wide variance in regional penetration of the social network Orkut,[20] popular in India and Brazil because of the large established base of users, yet almost unheard of anywhere else. Whether global or local, the combination of decreasing access costs with the growing value of access is a powerful engine for rapid global expansion of Internet users. The majority of cyber experts agree that "a global low-cost network will be thriving in 2020 and will be available to most people around the world."[21]

The need for a stable platform for software development acts against the forces driving large changes in existing devices and slows the introduction of new device classes. While hardware performance has shown exponential gains, the gains in software productivity are linear,[22] and it is these software tools and systems that must be optimized for each product class of end-user devices before sustainable market value is achieved. The economic value of stable platforms for development is enormous, preserving the continuity of existing product classes, since continuing compatibility generally has greater economic value than technological gains in efficiency or function.[23] Additionally, the time and effort required to establish and mature new software for a new type of cyber devices substantially slows the introduction and adoption of new product classes. The end result of these factors on the future is a strong force for the preservation of existing classes of cyber devices and the periodic introduction of new ones.

The future will see individuals using an increasing number of network-enabled devices, each optimized for the "human factors" related to the primary functions served by each device. The popular fascination with the phenomenon of ever-shrinking computing "boxes" with growing capabilities has led to repeated predictions of the "death of the desktop PC" by industry observers. What is often missed in the attention paid to increased sales of laptop computers is the steady sales of desktop computers. The well-worn narrative that recounts how giant mainframes were succeeded by business "mini-computer" servers, and then subsequent desktops, laptops, tablets, and smart phones, misses one crucial point. All of these product classes of computer systems still exist, just as predicted by "Bell's Law."[24] The key point to remember is new classes of endpoint computing devices complement the existing ones, they do not supplant them. This ever-increasing diversity of device types affects the qualitative character of cyberspace, by increasing the complexity of this ecosystem. Beyond the growing number of device types, another human factors consideration is the relative ability of a device to dynamically add new functionality.

This ability to add functionality is known as "generativity." Generativity is "a system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences."[25] In a generative system, third party software developers routinely offer new applications that users can select and load onto the device without the assistance or approval of the device creator.[26] This creates enormous economic value for both markets and individuals. Unfortunately, it also fundamentally depends on user permissions embedded in the device architecture that create system vulnerabilities which can’t be eliminated, only mitigated.[27] The other type of architecture is the polar opposite.

“Information appliances” are devices whose architectures are not user-extensible, and thus trade away flexibility and growth for increased simplicity, polish, and security. Blackberries, video game consoles, and “closed” mobile phones are all examples of information appliances, and they offer safer and more consistent experiences.[28] These “appliancized” devices are more limited and more secure than generative devices, and individuals are increasingly using a combination of both types of devices to access cyber-enabled functionality. An increasing number of traditionally closed appliances, vehicles, building systems, and personal articles will be invisibly connected to the Internet in order to improve their functionality, and this will alter the reach and characteristics of cyberspace. Creating the “Internet of Things” (IoT), these devices will be widely networked enabling them to be located, identified, monitored, and remotely controlled via the Internet. Despite an increased difficulty in recognizing security vulnerabilities in these systems, 50 to 100 billion devices will be connected to the Internet by 2020.[29, 30] The number of Internet nodes embedded in mundane objects may surpass the number of PCs and cell phones before 2035. As most of these cyber nodes will contain multiple sensors, the IoT will expand the reach, complexity, and vulnerabilities of cyberspace.

Future Cyber Networks

The individual networks and sub-internetworks that form the internet will be fundamentally transformed in the next 20 years. From a technical perspective, network technology is commonly associated with the five layers of the transmission control protocol/internet protocol (TCP/IP) model: the physical, data link, network, transport, and application layers.[31] The “application” layer is much larger than the rest, and can be viewed as having myriad layers itself.[32] One approach to rapidly implement new technologies is to create a separate network from the Internet. This approach creates gains in performance, functionality, and security at the cost of reduced connectivity and compatibility. An example is the “Internet2 Network” that provides a nationwide, high-speed network for its research, education, and industry members. It does not connect to the commercial Internet.[33] Alternatively, the “incremental fielding” approach involves periodic replacement of network infrastructure components with ones that incorporate newer technologies while preserving compatibility with older systems. Routers that handle both IPv4 and IPv6, and wireless access points that can operate in a mixed mode are examples. Future advances in the Internet will follow this path.[34] The result is the persistence of technical weaknesses and vulnerabilities inherent to superseded Internet technologies. While replacing the Internet with a new architecture would make it more secure, economic forces generally give more weight to interoperability and interconnectivity, which reduces costs, increases value to customers, maximizes network reach, and creates positive economic “network effects.”

Improving the economics by increasing interoperability and interconnectivity, often increases risk to individuals and organizations. One emerging approach involves the adoption of “Semantic Web” formats. The Semantic Web “provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries."[35] More generally, maximizing openness can increase risks to corporations to include theft of vital information (e.g., product technologies and customer data), compromise of internal communications, and disruption of critical processes. Given the value of information held in networks and the increasing number of process-control functions performed through them, Internet-linked networks are very attractive targets to wide variety of bad actors. This has led to an explosion in the number of network compromises in recent years, and the trends point to continued growth into the foreseeable future.[36]

One effective method to reduce this organizational risk is to segregate and isolate key functional networks. A "network security incident" is the term for a variety of technical actions that can lead to adverse network events.[37] Logically segregated networks reduce risk of these incidents through "walls" that provide barriers to access by non-authorized users. These barriers go beyond mere implementation of access controls, account permissions, or passwords, which are easy to bypass. True logical "segregation" of a network means that one or more protocol layers required for access are either proprietary or encrypted, and usually restrict access via proprietary client software. Traditionally, these segregated domains that exist on the Internet have been referred to as "walled gardens."

The strength of these walls varies based on the approach taken. Among the weaker approaches are those used by social networking sites. For sites like Facebook "each site is a silo, walled off from the others. ... This isolation occurs because each piece of information does not have a universal resource identifier. … So the more you enter, the more you become locked in."[38] The weakness of this approach is apparent in the amount of malware spread via Facebook phishing and redirects.[39] Other organizations with more to lose require stronger walls. One such example of a "strongly walled" network is Apple's iTunes system. One accesses iTunes only using Apple's proprietary iTunes program, which is technically not part of the Web. It is centralized and walled off.[40] Apple's economic incentive to prevent theft of its stored commercial media is clear. While user accounts are still compromised on occasion, these small losses are economically insignificant. As information of greater value becomes more common on the Internet, these logically walled network enclaves will rapidly proliferate.[41]

Moving a step beyond walled enclaves, logically isolated networks (isonets) create a separate logical network that leverages the infrastructure of the open Internet, while still being functionally closed off from it. These "virtual" networks rely on cryptographic tunneling protocols to preserve security while riding over the Internet. Virtual private networks (VPNs) utilizing point-to-point tunneling protocols are commonly used to implement organizational intranets that are logically isolated at numerous different levels throughout the Internet infrastructure using a wide variety of technologies. Logically isolated networks provide more protection than walled networks, and while advertised as secure, this is misleading. They are more secure, but common end-user devices (e.g. laptops) that connect to a VPN are subject to compromise via intercepting and manipulating link initiation messages to insert a covert node into the network. This approach is used by man-in-the-middle exploits.[42] In addition, disruption of the links identified by visible packet header information is a significant vulnerability. As above, the defensive strength of these logically isolated networks varies based on the technologies used. In general they provide significant protection against compromise, but only minor protection against network disruption.

Physically isolated networks are the most secure type of networks, and their cost is warranted for networks that control vital systems or contain highly sensitive information. These "pure" isonets are composed of cyber devices that have dedicated physical circuits, and no connections to any other network. The costs of building and operating such a network that is physically isolated are high, but may be warranted in special cases. Control networks for critical infrastructure such as utilities are referred to as supervisory control and data acquisition (SCADA) systems. These control networks, organizational networks that contain sensitive or classified information, and military command and control networks are among those that warrant this expense. Physically isolated networks provide the greatest degree of protection from both disruption and compromise, however, the number of these networks is actually decreasing due to IP convergence, IT cost cutting initiatives, and underestimation of risk by organizational leadership. The future will likely include numerous isonets driven by national laws and policies to increase protection, though this protection isn't perfect. Even critical networks that are designed to be completely isolated can be compromised. Network technicians under pressure may simply add "admin" connectivity to an intranet-linked computer to improve maintenance effectiveness, while losing isolation. Likewise, an expert user may physically connect a laptop with wireless connectivity to transfer data to the isonet, opening an exploitable wireless link. Indirect methods of compromise are also possible.

Even completely isolated networks are vulnerable to penetration by indirect methods such as USB-drive malware, social engineering methods, and covertly-emplaced devices. The publically-acknowledged penetration of US DoD computers by the virus "Agent.btz" demonstrated the ability of a cyber threat to bypass layers of logical security by leveraging user behavior to exploit security weaknesses.[43] More recently, Stuxnet demonstrated that sophisticated, targeted malware can penetrate truly isolated networks. Other social engineering techniques are used to trick users into circumventing network security,[44] and these techniques remain effective against isonets. The key point is that even pure isonets can be breached by the most capable of cyber actors.

Greater blurring of the work-leisure divide drives a need for synchronization between cyber devices, which increases information leakage from "closed" networks. Proliferation of smart phones and portable computers is driving the development of services that sync information between an individual's Internet services. Users increasingly seek seamless and instantaneous access to media and user-created content across all their cyber devices and services, increasing the digital presence of those using these services, and putting pressure on the integrity of closed and isolated networks.[45] Increasingly users are likely to establish ad hoc conduits to gain access to information they feel they need, resulting in “leakage” from organizational networks, reducing isonet and closed network security.[46]

User identification and authentication technologies will continue to grow until their use becomes pervasive by 2035 and anonymity will be costly to achieve and sustain.[47] As anonymity was the default in Internet design, identification and authentication had to be added later. Today, IP address tracking, use of “cookies” and persistent user IDs are means of identification.[48] However, one must be able to have confidence in the truth of these IDs, or the ability to “authenticate” them.[49] Since 2008, “federated authentication” systems have grown rapidly into a system of interlinked “identity providers” and “relying parties” through a variety of available products using the OpenID protocol.[50] The emerging Internet Protocol, IPv6, inherently contains an authentication function that “marks each packet with an encryption ‘key’ that cannot be altered or forged” which can be used to identify information senders and receivers.[51] Changes to the TCP/IP layers to further strengthen authentication and identification continue to be advocated, as commercial and government desires for increased security incentivizes the development of these technologies.[52] By 2035, individual anonymity that withstands the scrutiny of developed nation states is likely to exist only where it is engineered at significant cost, or where it is specifically protected by law.

Transparency

Current changes in cyberspace are resulting in greater visibility of all types of information, or “transparency,” which will cause profound change for individuals, organizations, and societies.

Transparency in this context means, “the quality of being characterized by visibility or accessibility of information.”[53] This informational transparency may enable transparency of personal activities and relationships, transparency that holds public officials accountable and fights corruption, and corporate transparency that provides accountability to stakeholders. This level of transparency will profoundly change our world and has significant implications for warfare.

The proliferation of location-aware public and personal sensing devices that connect to the Internet, will increase physical transparency. Internet-streaming cameras, whether in cell phones or as web cams, are increasingly commonplace, and are used for applications to include “nanny cams”, home security systems, store security, and traffic management systems. Future increases in the number, diversity, and resolution of these sensors, coupled with decreases in size and power footprints, will result in strong “locational” transparency well before 2035.[54]

Increasingly, cyber devices determine their physical location through global positioning systems (GPS), differential GPS, and cell tower “multilateration.” Indoors, Wi-Fi, Bluetooth, and RFID signals are often employed by devices to determine location where GPS and cellular reception can be problematic. Location-based services (LBS) such as navigation applications, finding nearby points of interest, and meeting the US/Canada “Enhanced 9-1-1” mandate all require cell phones to accurately display their location.[55]

While precise geo-location of an Internet device may require a user to operate either a web application or service that directly uses GPS, other methods do not require users to give permissions for their approximate location to be detected. The easiest method gain a device’s location is simply to query the device, but laws often require users to “opt-in” to a service that enables geolocation before this method can be used. This is usually done via the user clicking to “accept” the “terms and conditions” of a website or mobile application interface. While these terms are explicitly stated, many users fail to fully read them and do not realize what permissions they have granted.   The other common method for externally gaining a cyber device’s location is through “IP mapping,” which involves querying databases that match IP addresses to geographic locales, roughly accurate down to a single zip code.[56] This method is widely used by a variety of commercial and free location service provider application programming interfaces (APIs) and web sites, such as IP2Location, Google Geolocation API, and HostIP.info.[57] This latter method requires no approvals from users. These developments are resulting in increased transparency -- an ever-sharper two-edged sword for individuals.

Individuals

The same cyberspace functionality sought by businesspeople can enrich their personal lives, again at the cost of increased transparency.   Social interconnectedness can be enhanced among an individual’s family and friends through network-enabled devices and services. However, this increased transparency also means that as individuals use cyber devices, they leave “digital footprints” in cyberspace which are increasingly stored in databases.[58]   Systematic searches of these databases can yield an informational form of surveillance of individuals via cyberspace.[59] Even digital hermits will likely have a significant digital presence if they live within a modern community. Some who interact with these individuals will share information about these interactions. Further, device interactions inherent in the “Internet of Things” will record the digital footprints of passersby. Barriers to accessing this information mean that individuals are more likely to maintain their privacy vis-à-vis other persons than they are from corporations or against governments.[60] Meaningful individual privacy against *governments* will continue to degrade to the point where it only truly exists where it is deliberately maintained by law, markets, and architecture.[61] Regardless of the costs, a large and growing number of individuals are choosing to leverage cyberspace for personal and professional gains.[62]

Organizations

Growing cyberspace capabilities are yielding potential performance gains for organizations, though these gains come with intrinsic vulnerabilities. Organizations that strengthen information process management systems and then restructure to leverage their potential, gain improved performance and agility and deeper collaboration with partners. In business, these gains are evident in the results of outsourcing and global supply chains, where deep levels of collaboration are required.[63,64] In military organizations, this approach has resulted in achieving robust logistical sustainment of deployed forces, network-centric warfare, and time-sensitive targeting. Violent extremist organizations (VEOs) can leverage cyberspace to support dispersed groups through network-enabled recruitment, funding, training, and communications.[65]

Organizations leveraging cyberspace to realize gains in performance and agility increase their vulnerability to cyber warfare actions. The same information flows that enable strong collaboration and rapid execution necessitate external linkages, provide vectors for penetration. Even where these important networks are implemented as logically walled enclaves or isonets, risk is only partially mitigated and vulnerabilities remain. Further, organizational collaboration involved in such activities as outsourcing and supply chaining require more interconnectedness than just these segregated transactional networks. Planning between partners often results in links to key private data of the company and its partner organizations. Each of these links is a potential node for attack, whether the using organization is a company, VEO, or military unit.

[1] Dr. John P. Geis II, "The Age of Surprise," Presentation at the Air Education and Training Command Symposium, 23 January 2012.

[2] Tim Berners-Lee, "Long Live the Web: A Call for Continued Open Standards and Neutrality," *Scientific American*, December 2010, 1.

[3] Geis, 2012.

[4] Lee Rainie and Janna Anderson, "The Future of the Internet II," Pew Research Center Report, 24 September 2006, i-iii, http://www.pewinternet.org/Reports/2006/The-Future-of-the-Internet-II.aspx (accessed 8 February 2012).

[5] Lee Rainie and Janna Anderson, "The Future of the Internet III," Pew Research Center Report, 14 December 2008, 5, http://www.pewinternet.org/Reports/2008/The-Future-of-the-Internet-III.aspx (accessed 8 February 2012).

[6] Ibid., 6. There will be a modification of the current Internet structure, rather than a re-architecture of the whole system.

[7] Jonathan Zittrain, *The Future of the Internet—and How to Stop it* (Yale University Press, 2008), p. 8.

[8] Dr. Michio Kaku, *Physics of the Future: How Science Will Change Human Destiny and Our Daily Lives by the Year 2100* (New York: Doubleday, 2011), 20, 37-41. First stated in 1956, Moore's law simply says that computer power doubles about every eighteen months. The end of Moore's law has been predicted numerous times, but it has held true for more than fifty years.

[9] Ibid., 37-41. Physicist Michio Kaku predicts that Moore's law will hold true until shortly after 2030, when silicon processors will be replaced by another technology, and processing power will grow at a much slower pace thereafter.

[10] Recent analysis predicts that Moore's Law will hold true for CMOS technology through 2024. Candidates to replace CMOS include spintronics, nanowires, nanotubes, graphene, and other more exotic technologies. These are all being tested in the research labs, but none are ready to provide a wholesale replacement of CMOS. To that end, one of the principal recommendations of the authors is for more government funding to accelerate the evaluation, research and development of these technologies, as a precursor to commercial production 10 to 15 years down the road. See: Mark Snir, William Gropp, and Peter Kogge, "Exascale Research: Preparing for the Post-Moore Era," 19 June 2011, http://www.ideals.illinois.edu/bitstream/handle/2142/25468/Exascale%20Research.pdf (accessed 12 February 2012).

[11] Gilder's Law states that network bandwidth triples every 18 months. See: Dion Hinchcliffe, "Twenty-two power laws of the emerging social economy," 5 October 2009, available at: http://www.zdnet.com/blog/hinchcliffe/twenty-two-power-laws-of-the-emerging-social-economy/961 (accessed 12 February 2012).

[12] Kryder's Law says that magnetic disk areal storage density doubles approximately every 18 months. See: Chip Walter, "Kryder's Law," *Scientific American*, 25 July 2005, available at: http://www.scientificamerican.com/article.cfm?id=kryders-law (accessed 12 February 2012).

[13]Gordon Bell's Law states that "established market class computers are introduced at a constant price with increasing functionality (or performance), and technology advances in semiconductors, storage, interfaces and networks enable a new computer class (platform) to form about every decade to serve a new need." Each new usually lower priced class is maintained as a quasi independent industry (market). Classes include: mainframes (60's), minicomputers (70's),

networked workstations and personal computers (80's), browser-web-server structure (90's), web services (2000's), et cetera. See: http://research.microsoft.com/en-us/um/people/gbell/ (accessed 12 February 2012).

[14] Marc Andreessen, interview by Charlie Rose, *Charlie Rose Show*, MSNBC, 19 February 2009.

[15] Rainie and Anderson, 2008, 5-10.

[16] Vinton Cerf, in an interview called "The Future of the Internet," *Gallop Market Journal*, 13 April 2006. Available on-line at: http://gmj.gallup.com/content/22348/future-internet.aspx#2 (accessed 8 February 2012).

[17] More technically, the term "network effect" can be defined as "a change in the benefit, or surplus, that an agent derives from a good when the number of other agents consuming the same kind of good changes." See: S. J. Liebowitz and Stephen E. Margolis, "Network Externalities (Effects)," *The New Palgrave's Dictionary of Economics and the Law* (MacMillan, 1998).

[18] This positive network effect is also reflected in "Metcalf's Law": Utility of a network is proportional to the square of the number of users. See: Hinchcliffe, "Twenty-two power laws of the emerging social economy," 2009.

[19] A precise definition of "local network effect" is the situation where "rather than valuing an increase in the size of a product's user base or network in general, each agent values adoption by a (typically small) subset of other agents, and this subset varies across agents." See: Arun Sundararajan, "Local Network Effects and Complex Network Structure," *The B.E. Journal of Theoretical Economics*, 2007, Vol. 7, Iss. 1, Article 46.

[20] Local network effects explain why Orkut is extremely popular in Brazil and India – but is nearly unheard of in the U.S. See: Matt Peterson, "Orkut Dissected: Social Networking in India & Brazil," 27 June 2011, http://www.aimclearblog.com/2011/06/27/orkut-dissected-social-networking-in-india-brazil/ (accessed 12 February 2012).

[21] Rainie and Anderson, 2006, 5-6.

[22] Vu Nguyen, LiGuo Huang, and Barry Boehm, "An Analysis of Trends in Productivity and Cost Drivers over Years," 2010, available at: http://csse.usc.edu/csse/TECHRPTS/2010/usc-csse-2010-521/usc-csse-2010-521.pdf (accessed 12 February 2012).

[23] Andreessen, *Charlie Rose Show*, 2009.

[24] Gordon Bell's Law (as noted above) holds that each new computer class (platform) is maintained as a quasi independent industry (market). See: http://research.microsoft.com/en-us/um/people/gbell/ (accessed 12 February 2012).

[25] Zittrain, *Future of the Internet*, 70.

[26] Ibid., 70-71, 86-89.

[27] Ibid., 99-102. The ability of users to dynamically add new functionality to a cyber device requires a significant degree of system-level authority to be granted to the user. These generative systems can attempt to prevent the user from choosing to run compromised or malicious code, but in the end it remains the individual's choice.

[28] Ibid., 13, 17-18, 58-59.

[29] Harald Sundmaeker, et al. (eds.), *Cluster of European Research Projects on the Internet of Things (CERP-IoT): Vision and Challenges for Realising the Internet of Things*, (Brussels, 2010), 12-31.

[30] National Intelligence Council, "Conference Report: Disruptive Civil Technologies, Six Technologies with Potential Impacts on US Interests out to 2025," Presented at the Disruptive Civil Technologies Conference, 10 April 2008.

[31] Siyan Karanjit, *Inside TCP/IP*, New Riders Publishing, 1997.

[32] Zittrain, *Future of the Internet*, 67-70.

[33] Internet 2 Fact Sheet, http://www.internet2.edu/resources/AboutInternet2.pdf (accessed 8 February 2012).

[34] 78% of experts agree (vs. 6% who disagree) that "next-generation research will be used to improve the current Internet; it won't replace it." See: Rainie and Anderson, 2008, 6-8.

[35] W3C Semantic Web Activity web site available at: http://www.w3.org/2001/sw/ (accessed 8 February 2012).

[36] Data on unique malware variants compiled by AV TEST Institute shows explosive growth over the past fifteen years, with a particular acceleration starting in 2006, showing less than 3 million malware variants, through 2011, when there were approximately 65 million. Charts available at: http://www.av-test.org/en/statistics/malware/. For more detailed analysis see: http://www.securelist.com/en/analysis/204792162/Kaspersky_Security_Bulletin_2010_Statistics_2010 and http://press.pandasecurity.com/wp-content/uploads/2012/01/Annual-Report-PandaLabs-2011.pdf, with predictions at: http://www.sans.edu/research/security-laboratory/article/security-predict2011 (accessed: 11 February 2012).

[37] A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. See: NIST Special Publication 800-61, section 2.1, http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf (accessed 11 February 2012).

[38] Berners-Lee, "Long Live the Web," 3.

[39] Georg Wicherski, "The Dangers of Social Networking," Kaspersky Lab SecureList Analysis, 19 April 2010, http://www.securelist.com/en/analysis/204792113/The_Dangers_of_Social_Networking (accessed 11 February 2012).

[40] Berners-Lee, "Long Live the Web," 5.

[41] Rainee and Anderson, 2008, 2-8, 32.

[42] Peter Burkholder, "SSL Man-in-the-Middle Attacks" (SANS Institute, 2002), available at: http://www.sans.org/reading_room/whitepapers/threats/ssl-man-in-the-middle-attacks_480 (accessed on 14 February 2012).

[43] Kim Zetter, "The Return of the Worm That Ate the Pentagon," *Wired*, available on-line at: http://www.wired.com/dangerroom/2011/12/worm-pentagon/ 9 December 2010; Nakashima, "Cyber-intruder sparks massive federal response — and debate over dealing with threats," *The Washington Post*, on-line at: http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_print.html, 8 December 2011; William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010;

[44] By definition, developing a relationship with a user in order to unwittingly trick them or get them to do something which undermines network security is called "social engineering." See: Malcolm Allen, "Social Engineering: A Means to Violate a Computer System" (SANS Institute, 2007), available at: http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violate-computer-system_529 (accessed on 14 February 2012).

[45] In this context, a “closed” network is refers to a network to which access is only allowed to users who have been authenticated.

[46] Rainie and Anderson, 2008, 6, 16-17.

[47] For the purposes of this paper, “user identification” refers to both the identity of the user and a collection of “identifiers” of that user (i.e., name, date of birth, address, and driver’s license number, etc…).

[48] Renata Ivancsy and Sandor Juhasz, "Analysis of Web User Identification Methods," *World Academy of Science, Engineering and Technology*, 2007, Vol. 34, 338-340, available at: www.waset.org/journals/waset/v34/v34-59.pdf (accessed 18 January 2012).

[49] Authentication is defined as the ability to gain truth about an asserted claim, such as the validity of a user ID or request for information. See: Lawrence Lessig, *Code version 2.0*, (New York: Basic Books, 2006), 40.

[50] Wesley Chun, “Using Federated Authentication via OpenID in Google App Engine,” July 2010, http://code.google.com/appengine/articles/openid.html (accessed on 18 January 2012).

[51] Lessig, *Code version 2.0*, 54.

[52] Corporations seek better security for information of monetary value; repressive governments often seek the ability to control information flow within their sovereign spaces. Collectively, these two forces drive the development and proliferation of additional security technologies. See: Lessig, *Code version 2.0*, 50-58.

[53] Webster’s New Collegiate Dictionary, 1242.

[54] Increases in the number, diversity, and resolution of networked digital sensors, is resulting in growing locational transparency now, prompting security concerns by many. This trend shows no sign of stopping. See: Roger Clarke and Marcus Wigan, “You Are Where You’ve Been: The Privacy Implications of Location and Tracking Technologies”, *Journal of Location Based Services*, December 2011, Vol. 5 Issue 3-4, 138-155.

[55] By law within the U.S. and Canada, 67% of all phones must be locatable within a radius of 100 m and 90% must be within 300 m. See: http://www.fcc.gov/rulemaking/07-114 (accessed on 30 January 2012).

[56] Lessig, *Code version 2.0*, 58-59.

[57] For further details, see such websites as: *www.fraudlabs.com/ip2location.aspx* , *code.google.com/apis/gears/api_geolocation.html, and www.hostip.info*.

[58] Roger Clarke, “The Digital Persona and its Application to Data Surveillance”, *The Information Society*, June 1994, Vol. 10 Issue 2.

[59] Clarke and Wigan, “You Are Where You’ve Been,” 138-155. See also: Lessig, *Code version 2.0*, 206-7.

[60] Rainie and Anderson, 2010, 43. Reference comments attributed to Bernie Hogan.

[61] Lessig, *Code version 2.0*, 223.

[62] Facebook alone had 845 million monthly active users as of 31 December 2011, a substantial increase over the 608 million one year earlier. See: Facebook S-1 SEC Filing, 1 February 2012, 1, http://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287 (accessed: 4 February 2012).

[63] Friedman describes the trends of outsourcing, global supply chains, and “insourcing,” as well as the resulting competitive advantages. See: Thomas L. Friedman, *The World is Flat: A Brief History of the Twenty-first Century*, 3rd ed. rev. (New York: Picador, 2007), 126-168.

[64] For a discussion on the deep level of collaboration required in "insourcing" (strong-form outsourcing) as well as "just-in-time" global supply chaining, see: Friedman, *The World is Flat*, 151-154, 169-171.

[65] A report entitled "Examining the Cyber Capabilities of Islamic Terrorist Groups" by Andrew McPherson of Dartmouth College in 2004, found five areas where there is clear, factual evidence that Islamic terrorism is flexing its muscles in the cyber realm. These areas are: 1. Propaganda, 2. Recruitment & Training, 3. Fundraising, 4. Communications, and 5. Targeting. The report provides examples and analysis for each area. Available at: http://www.ists.dartmouth.edu/docs/ITB_032004.pdf (accessed 12 February 2012).

Cyber Warfare Capabilities in 2035

Over the next two decades, classes of militarily significant adversaries will remain largely unchanged, however, their capabilities and vulnerabilities will likely be very different. The militaries of regionally dominant nation-state adversaries will increasingly leverage cyberspace to implement network-centric warfare capabilities (e.g., A2/AD) and to extend their operational reach. Growing numbers of VEOs will leverage commercial network and device capabilities to improve mobility and reach, and to enable decentralized operations to evade detection and limit the damage of counterstrikes. While these approaches substantially marginalize traditional military capabilities, they are particularly vulnerable to cyber warfare capabilities.

ISR

Military cyber intelligence, surveillance, and reconnaissance (ISR) capabilities will leverage increasing informational transparency to detect, identify, penetrate, map, exploit, target, and track adversary organizations and assets. Although coercive organizations will maintain cyberspace constructs that preserve opacity, strong transparency mechanisms will enable detection from a single event. This single detection will be increasingly likely to result in an individual's identification. Discovery and penetration of that individual's cyber devices will enable the mapping and exploitation of the logical, physical, and social networks of the adversary organization. Additionally, cyber ISR assets will be able to perform logical and physical tracking of targeted individuals and assets. Dynamic target location can later be sent to weapon systems for action. While this may be a bomber, it might also be an offensive cyber weapon system.

Disrupt

Future offensive cyber warfare systems will utilize attack techniques against adversary cyber devices and networks to create a variety of functional effects, from short-term disruption to physical destruction or purposeful influence. These cyber warfare "functional effects" are analogous to conventional "kill mechanisms."[1] The simplest warfare functional effect in cyberspace is deliberate *disruption* of inter-nodal information flows, requiring only the logical address(es) of the target and a means of access. One example of this approach is "distributed denial of service" (DDoS) attacks employed by "hacktivists" against web sites of targeted companies.[2] Disruption attacks result in informational isolation, which causes loss of tactical situational awareness and coordination. Importantly, these attacks can negate network-centric warfare capabilities entirely. Note that disruption can be effective without knowing the physical location of the target(s). The duration is generally counted in hours, but may last for many days against unprepared target organizations.[3] As effective as disruption is, more versatile effects are possible with more sophisticated methods.

Deceive

A more advanced cyber warfare effect is deception, which manipulates adversary information systems by presenting an altered view of the external environment. Deception of the automated decision-making logic within cyber devices is commonly referred to as "spoofing."[4] The minimum threshold for machine-level deception requires logical access, the ability to negate or "override" the true logic stream(s), and knowledge of the data structure formats used by the targeted link(s). Logically breaching the device is not required. This attack method will require more preparation than simple disruption. Functional effects will range from simple misdirection to the indirect control of autonomous vehicles or control systems. Duration of the effect will depend on the degree of human monitoring and the existence of override controls in the target system, but could be expected to last from minutes to hours. As tactically significant as deception may be, breaching a cyber device opens greater possibilities.

Disable

A more persistent effect involves *disabling* or "blanking" a cyber device, which entails breaching a device and altering its system-level core logic to make it functionally useless. Examples of specific methods include deleting key operating system files, or corrupting the BIOS. The result is roughly equivalent to a conventional "functional kill" mechanism, though in cyberspace physical damage is unnecessary to achieve this effect. Instead, it will generally involve breaching the device, gaining system-level privileges, and then executing a payload. An example of this functional effect is the "bricking" of cell phones.[5]   Duration of the effect will depend on the availability of maintenance services, but could be expected to last days to weeks. By 2035, this attack method could have the potential to paralyze entire military units or disable critical infrastructure systems. As powerful as blanking will be, cyber warfare effects won't peak there.

Control/Destroy

The strongest functional effect in cyber warfare is *control*, though it is also the hardest to achieve. Control of a cyber device generally involves overwriting specific areas of application layer code in a way that enables subversion of function by the attacker. This control can involve either live commands or pre-programmed instructions. Further, once control is gained over a device, that control may remain passive until activated for a specific purpose later. One example is a personal computer compromised by malware to become a botnet "zombie."[6] The Stuxnet worm also achieves this effect.[7] The level of control need not be total, only sufficient to direct the intended action(s). Control will often enable physical destruction of the device, as well as all other functional cyber warfare effects. Duration will be driven by the degree of device security, but could be expected to last minutes to hours after active control is asserted. Duration on devices with weak security could last indefinitely. In the next two decades, cyber attack systems will be increasingly capable of hijacking the weapon systems and control networks. Unmanned aerial vehicles will be particularly vulnerable to hijacking due to numerous factors. By 2035, cyber attack is likely to be capable of destroying many military vehicles and infrastructure systems directly, and under certain circumstances to cause autonomous weapon systems to attack their owners.

Message

The final cyber warfare effect is *messaging*, which leverages cyber communication channels to carry informational messages to specific individuals or audiences. Over the past twenty years, the number and diversity of digital communication and media channels travelling over the Internet has exploded. In conjunction with advanced electronic warfare (EW) platforms, cyber warfare platforms are well-suited to perform in a "precision message delivery" role for influence operations (IFO). This form of EW capability has been a traditional USAF mission.[8] Within this context, cyber warfare platforms can serve as the "hardware" for IFO "software" during influence missions.[9] As digital communication conduits proliferate, adding messaging capabilities to cyber warfare systems will pay increasing dividends for the effectiveness of joint influence operations. In the future, cyber warfare messaging effects will be capable of messaging specific individuals through multiple, different communication services in a highly controlled manner. Conversely, it will be possible to convey messages to any subset of combatants identifiable by intelligence.

[1] Conventional kinetic "kill mechanisms" are found in the joint munitions effectiveness manual (JMEM). See: www.weaponeering.com/jtcg_me_history.htm (accessed 12 February 2012).

[2] 2011 saw a high number of attacks against corporations by "hacktivists" DDoS-ing sites for political and ideological motives. See: "Arbor Special Report: Worldwide Infrastructure Security Report VII, 2011," 7 February 2012, http://arbornetworks.com/report (accessed 12 February 2012).

[3] Disruptive DDoS attacks lasted for several weeks against Estonia in April 2007, and were effective for much of this time window. Similar effects were experienced by the nation of Georgia in 2008. See: Martin Libicki, *Cyberdeterence and Cyberwar*, (Santa Monica, CA: RAND Corporation, 2009), 1-2.

[4] One dramatic example of spoofing a cyber system occurred mid-June of 2011, when a hacker broke into the "bitcoin" virtual currency exchange based in Tokyo and spoofed the system by simulating a massive sell-off, driving the exchange rate toward zero, and allowing him to acquire 2,000 bitcoins (worth over $40,000 at the time) for virtually nothing. See: Benjamin Wallace, "The Rise and Fall of Bitcoin," *Wired*, December 2011, 107.

[5] The term "bricking" is defined placing a piece of equipment into a hung, wedged, or unusable state through programming or configuration actions. Especially used to describe what happens to devices like routers or PDAs that run from firmware when the firmware image is damaged or its settings are somehow patched to impossible values. This term usually implies irreversibility, but equipment can sometimes be "unbricked" by performing a hard reset or some other drastic operation. See: http://www.catb.org/jargon/html/B/brick.html (accessed: 12 February 2012). Senator Chuck Schumer made news in August 2011 when he "asked wireless companies to do more than disabling a stolen phone's SIM card…wants the whole phone bricked so it can never be used again." See: http://consumerist.com/2011/08/senator-wants-wireless-companies-to-do-more-to-disable-stolen-phones.html and http://articles.nydailynews.com/2011-08-21/news/29933555_1_cell-phones-phone-companies-at-t-store.

[6] A "botnet" (roBOT NETwork), is a large number of compromised computers ("zombies") that are used to generate spam, relay viruses or flood a network or Web server with excessive requests to cause it to fail (see denial of service attack). The computer is compromised via a Trojan that often works by opening an Internet Relay Chat (IRC) channel that waits for commands from the person in control of the botnet. There is a thriving botnet business selling lists of compromised computers to hackers and spammers. Source: http://www.pcmag.com/encyclopedia_term/0,2542,t=botnet&i=38866,00.asp (accessed 12 February 2012).

[7] The Stuxnet worm took control of computers linked to uranium-enriching centrifuges and damaged an estimated 5,000 of them to the point that they had to be replaced. See: "PandaLabs Annual Report – 2011," 10.

[8] This role of special-purpose EW aircraft providing a psychological operations broadcast capability has been a traditional USAF mission, performed first by the EC-121 Coronet Solo, then the EC-130E Volant Solo, and now the EC-130J Commando Solo aircraft. See: "USAF Fact

Sheet on EC-130J Commando Solo," http://www.af.mil/information/factsheets/factsheet.asp?id=182 (accessed: 6 February 2012).

[9] Colonel Randolph Rosin, "To Kill a Mockingbird: The Deconstruction of Information Operations," *Small Wars Journal*, 17 August 2009, 8, http://smallwarsjournal.com/jrnl/art/the-deconstruction-of-information-operations (accessed 6 February 2012).

Cyber Weapon Systems

In militaries across the world (and in the USAF in particular), "weapon systems" are the predominant construct for fielding and sustaining viable warfighting capabilities,[1] and this is the natural path forward for cyber. Weapon systems are composed of several key elements. First, a weapon system includes mission equipment, both hardware and software components. Second, a weapon system includes trained and qualified mission-ready personnel, as well as dedicated mission support personnel who perform such tasks as system maintenance or generating intelligence products. Finally, mission essential supplies are also included, such as spare parts and munitions.

Distinctive Characteristics

A few characteristics are distinctive of cyber weapon systems, as opposed to air or space systems. First, the mission system is highly modular, changes relatively often, and can be geospatially dispersed. Its "logical" construction and capabilities are what make it a weapon system. Its physical components largely mirror those of cyber infrastructure systems. These weapon systems are not built in "blocks", but rather grown perpetually via rapid increments. A second characteristic is the access mechanism to the operational environment--cyber weapon systems require one or more "domain access points" that provide persistent connectivity.[2] The resilience of a cyber weapon system is largely dependent on its access point(s). Finally, cyber munitions are extremely specialized, and are often tailored for each individual target or environment. These cyber munitions are generally analogous to an offensive variant of AFRL's "Cybercraft" concept.[3] As adversaries respond to attack, the cyber munitions must be rapidly reprogrammed to maintain tactical effectiveness during an operation. This is manpower intensive and requires network attack coders to be embedded in these operations squadrons.[4]

Automation

The difficulty of achieving automation and autonomous decision-making engines in cyberspace weapon systems will prove to be much greater than for any other domain. The heterogeneous and dynamic characteristics of the cyber domain make automation susceptible to rapid obsolescence. The fundamental challenge for automation in cyber weapon systems is that the very high level of complexity and volatility in cyberspace (described above) makes fully automating offensive and defense systems impossible for the foreseeable future. While basic automation will be inexpensive, development of a highly automated system able to responsively adapt to a volatile tactical environment would be extremely expensive, even before anything approaching an effective autonomous cyber weapon system is realized. Nevertheless, automation is a crucial tool in the management and defense of large networks, and is therefore achieved even when the cost is high. This form of automation involves the near-continuous monitoring and reprogramming of expert systems by highly-trained professionals who chase down discrepancies between expert system predictions and actual events.[5] This type of system also represents an ideal case, since the networks being automated are the company's own.

Achieving a comparable level of automation while operating in "other people's networks" is even more difficult. Automated tools for probing, mapping, and breaching are less effective than generally understood,[6] and this limitation will continue to hold. Achieving even modest gains in automation within cyber weapon systems will require greater emphasis on human-machine interfaces.

Mission Crew

When considered together, the dynamic and heterogeneous nature of cyberspace, combined with the difficulty of achieving strong automation, means that mission operators will remain the core of effective cyber weapon systems well past 2035. Weapon systems will be formed around mission crews consisting of operators who specialize in various "network classes," led by a crew commander possessing tactical engagement skills, and supported by on-call rapid reprogramming engineers.[7] These crews must be capable of performing small alterations to automated functions in rapid iteration during missions, and linking to reprogramming engineers when stymied. Given the trends in complexity and volatility, it is doubtful that a "single-seat" cyber weapon system will be any more militarily significant than a single-seat motor boat is to today's navies—it may have ISR utility, but little else.

Synchronization/Integration

Cyber warfare capabilities are well-positioned to draw upon deep and diverse situational awareness sources through cyberspace, and then utilize speed-of-light attacks in synchronization and integration with other force elements. Situational awareness in cyberspace depends on a robust sensor subsystem in the weapon system itself, coupled links to a diverse set of dynamic databases to create a multi-dimensional tactical and operational "picture." Tactical synchronization with cyber defense weapon systems will prove crucial to identifying and countering adversary cyber attacks, and will rely upon the relative robustness of tactical datalinks between platforms. Robust datalinks will enable millisecond tactical synchronization, as well the ability to perform cyber warfare actions tunneled through air and space vehicles with advanced electronic attack capabilities. This "air and space enabled cyber warfare" has particular potential for countering future A2/AD capabilities.

Stealth

As cyberspace is an engineered domain, stealth is easier to achieve there than in physical space, and given the potential for covert attack in this domain, it is valuable as well. Anonymity was enabled by the original Internet architecture, so few worry about "stealth" in cyberspace. Those who are concerned with preserving anonymity can use a variety of free Internet "anonymizer" services.[8] Increasing transparency and attribution in the cyber domain will raise the bar for achieving stealth. In the future, the level of cyber stealth now achieved by skilled individuals will require the expertise and resources of major corporations, or governments. Beyond the tactical utility, stealthy cyber weapon systems could provide additional strategic options in response to covert cyber attacks by adversaries.[9] Further, stealthy cyber weapon systems exercise selective "self-attribution," depending on the mission's aim.

[1] The formal definition of a "weapon system" is found in Joint Pub 1-02, and reads, "A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency."

[2] The "domain access points" for cyber weapon systems can be thought of as roughly parallel to airfields for aircraft, or launch vehicles and ranges for spacecraft. There are two notable differences. First, a domain access point must remain functional in order for the cyber weapon system to operate in the wider cyberspace environment. Second, a cyber weapon system may be composed of multiple domain access points, which may be used simultaneously or in sequence, depending on the mission system architecture and mode.

[3] William Berry and Cheryl Loeb, "Breakthrough Air Force Capabilities Spawned by Basic Research" (National Defense University, 2007), 20.

[4] Timothy P. Franz, "IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way-Ahead for Network Warfare Forces" (AFIT, March 2007), 98.

[5] The AT&T Global Network Operations Center (GNOC) is an example of such a system. At the heart of the GNOC is a group of highly-trained professionals who chase down discrepancies between expert system predictions and actual measurements, write and test new rules for the expert system, and then upload the new rule set into the automated expert system. This is a man-on-the-loop instead of a man-in-the-loop system, but the "man" is an expert himself, and is watching the loop with great attentiveness, with on-site reprogramming capability readily available. See: http://www.corp.att.com/gnoc/ and http://blog.laptopmag.com/a-look-at-the-heart-of-att (accessed on 12 February 2012).

[6] The relative weakness of automated cyber vulnerability tools is highlighted, and specific effectiveness numbers are cited in a recent presentation at a Usenix conference. See: Dave Aitel,

"Three Cyber War Fallacies," (Usenix 2011, 9 August 2011), http://prezi.com/wdqab38lxr89/three-cyber-war-fallacies-usenix-2011/ (accessed on 14 January 2012).

[7] Franz, "IO Foundations to Cyberspace," 94-98.

[8] For an explanation of how Internet "anonymizer" services work, as well as a listing of the more popular ones, see: http://www.livinginternet.com/i/is_anon_work.htm and http://searchsecurity.techtarget.com/definition/anonymous-Web-surfing.

[9] When facing a covert cyber attack by an adversary, stealthy cyber weapon systems provide national leadership with the option for a covert response. Libicki refers to covert cyber espionage and attack actions as *sub rosa* actions. He goes on to describe a range of possibilities, from individual *sub rosa* attacks to full *sub rosa* cyberwar. He further details the likely pros, cons, and implications of this approach. However, because Libicki assumes that cyber attribution will not get any easier in the foreseeable future, he does not factor stealth into his deliberations. See: Libicki, *Cyberdeterence and Cyberwar*, 49, 94-102, 128-129, and, Martin Libicki, "Pulling Punches in Cyberspace," *Proceedings of a Workshop on Deterring Cyberattacks* (Washington, DC: The National Academies Press, 2010), 130, 136-139, available at: http://www.nap.edu/catalog.php?record_id=12997 (accessed on 12 February 2012).

Future Cyber Capabilities in Global Strike

One core capacity of the USAF is "global strike," the ability to quickly and precisely attack any target anywhere, anytime. A global strike mission is commonly intended to produce a direct strategic effect on an adversary center of gravity.[1] While the term global strike generally invokes thoughts of bombers and ICBMs, global strike really consists of a family of integrated lethal and non-lethal capabilities, which influence the strategic behavior of potential adversaries by holding key targets at risk.[2] Cyber warfare capabilities will be vital to ensuring the USAF can hold any target across the globe at risk in the year 2035.

While global strike missions may be aimed at "any target anywhere," some examples of potential adversaries and target classes in the year 2035 will help illustrate cyber warfare's probable roles. Potential nation-state adversaries studied in the USAF Blue Horizons program using the "alternate futures" methodology include a "resurgent Russia," a "peer China," a Jihadist Insurgency, and a "failed Nigeria."[3] Representative target classes for these global strike scenarios include military command and control systems, advanced air defense systems, critical infrastructure control systems, VEO leadership hiding in urban areas, and cyber criminal organizations raiding American corporations from a nation-state sanctuary.

Scenario One

In the year 2036, conflict between China and the Philippines over ownership of the Spratly Islands resulted in naval confrontations (see Figure 1).[4] Eventually, one encounter turned violent. A Filipino frigate was damaged and a Chinese destroyer was sunk. The situation escalated to the point where several Filipino aircraft were shot down by advanced SAM batteries operating in the Paracel Islands. After another naval engagement, the PRC

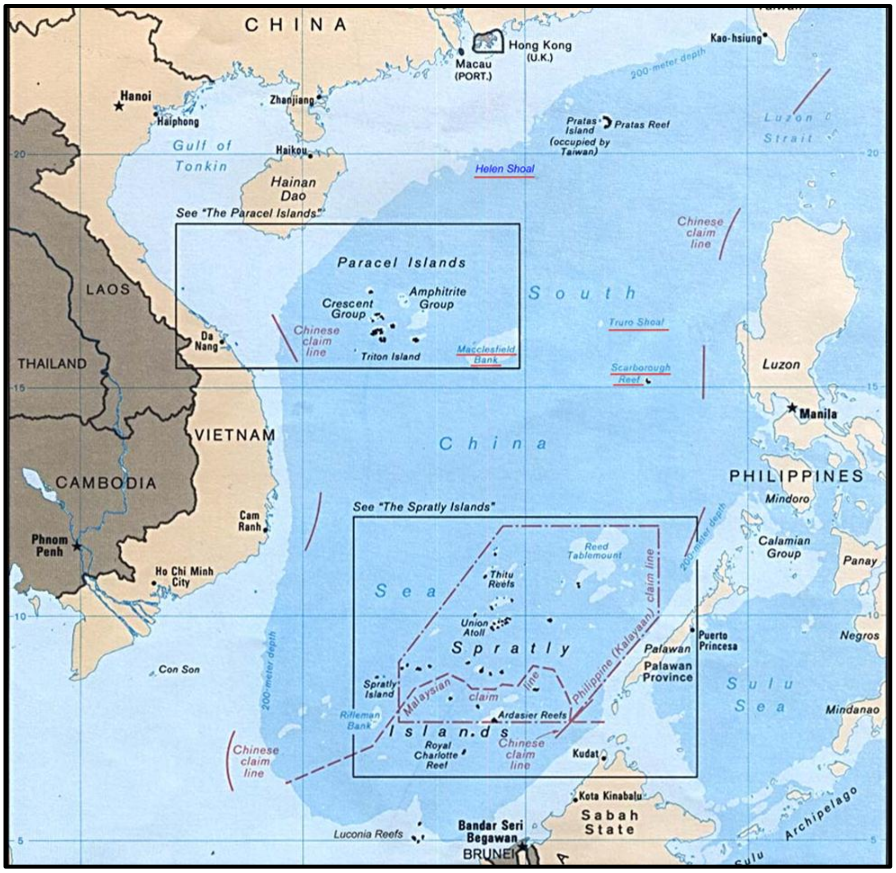

Figure 1: South China Sea

launched several ballistic missiles, striking the Philippine Island of Palawan. As a result, the Philippine Government invoked the 1952 U.S.-Philippines Mutual Defense Treaty.

Shortly thereafter, POTUS ordered a rapid global strike operation to degrade PRC offensive capabilities in the area, and to demonstrate resolve. During this operation, USAF cyber weapon systems played several roles. First, *disruptive* cyber attacks isolated the PRC area denial capabilities, allowing strike and electronic attack aircraft to destroy the SAMs operating on the Paracels. Next, cyber warfare systems *disabled* the fuel distribution system at the closest naval port on the Chinese mainland. This was accomplished by seizing logical *control* of its SCADA network nodes, *destroying* a few key valve and pump motors through over-cycling them, and then *disabling* sensor and controller logic units. Finally, these cyber warfare platforms performed a *messaging* action, placing a Chinese language video documentary on the Tiananmen Square historical incident prominently on the personal computers of local government officials. The result was a cessation of military hostilities with an increase of rhetoric from the PRC leadership, followed a few days later by quiet coordination for state-to-state negotiations.

Scenario Two

In the year 2037, a jihadist insurgency operating against monarchies on the Arabian Peninsula fomented unrest among significant portions of the citizenry. The insurgent leader was a particularly charismatic individual, and his steady stream of short videos resonated with many dispossessed youth. Fearing that the presence of US forces would further inflame the situation, these nations requested American military assistance, but implored that US forces not use bases on the peninsula. US Cyber ISR capabilities parsed an enormous quantity of video, identifying several insurgents. The social networks of the insurgency were then *mapped* through cyberspace, identifying the insurgent leader and his inner circle. Their cyber devices enabled continuous physical *tracking* of the insurgent leader. Several days later, the insurgent leader left the city in the middle of the night in a heavily armed convoy, bound for another city four hours away. Halfway into the trip, a USAF cyber weapon system took active *control* of the insurgents' covertly compromised cell phones. It then *disabled* all four vehicles by *blanking* the engine control units through a digital link intended for remote maintenance diagnostics, and then continuously passed coordinates of the insurgents to the stealth attack aircraft as they struck out on foot. None of the insurgents saw another sunrise. These two scenarios offer insight into unique and complementary roles that future cyber capabilities could perform in global strike missions.

[1] United States Air Force, *Air Force Doctrine Document 1 (AFDD-1)*, 14 October 2011, 26.

[2] General Norton A. Schwartz, Chief of Staff of the United States Air Force, Speech at the Air Force Association Luncheon at Maxwell Air Force Base, Alabama, 25 January 2012.

[3] John P. Geis II, Christopher J. Kinnan, Ted Hailes, Harry A. Foster, and David Blanks, *Blue Horizons II: Future Capabilities and Technologies for the Air Force in 2030*, (Maxwell Air Force Base: Air University Press), July 2009, 3-20.

[4] Map of South China Sea, 1988, Author: US Central Intelligence Agency, available at: http://en.wikipedia.org/wiki/File:Schina_sea_88.png accessed on 13 February 2012. This image is a work of a Central Intelligence Agency employee, taken or made during the course of the person's official duties. As a work of the United States Government, this image or media is in the public domain.

Conclusion

Future cyber warfare systems hold great potential to generate unique capabilities that strongly compliment air and space weapon systems, but realizing this potential requires an appreciation of the key challenges. First, the speed of execution in cyberspace is so fast as to require automation, but the environment's growing complexity and volatility limits automation to amplifying the tactical effectiveness of well-trained cyber warriors. Meaningful machine autonomy in cyber warfare is beyond 2035, if even then. Second, against a creative adversary, the uncertainty of warfare reduces the effectiveness of automation in cyberspace, so cyber warfare will be more manpower intensive than is commonly understood. Third, the volatility inherent in cyber warfare necessitates a rapid reprogramming system for cyber sensors, defenses, probes, and munitions.

Overcoming these challenges to achieve the desired cyber capabilities requires adopting a weapon systems approach for cyber warfare systems, and implementing it with the vigor the USAF shows for air and space vehicles. This includes several key elements, starting with the need to establish cyber warfare program lines, completely separate from cyber infrastructure ones. Next, research and development must directly address cyber weapon system technology shortfalls, and be made more robust. Further, the AF must expand the training and education programs aimed at building the tactical and operational effectiveness of cyber warriors. Finally, a cyber crew force management policy is needed, one that purposefully manages the small pool of cyber warriors. Only by doing all of these things can the AF build the needed cyberspace capability to conduct global strike -- anyplace and anytime.

These cyber warfare systems will possess near-instantaneous ability to strike stealthily across the globe, inflicting effects variable in both lethality and area. Global strike roles for future cyber weapon systems include: negating adversary A2/AD capabilities; disabling militarily significant infrastructure control systems; enabling targeted influence operations; performing ISR to detect, map, and track violent extremists; and countering pirates and privateers raiding American commercial organizations from nation-state sanctuaries. The alternative to driving toward these cyber capabilities is to "accept risk," hoping that perhaps other kinetic technologies will negate adversary A2/AD challenges, and hoping conventional strike capabilities will deter potential adversaries from employing covert cyber attacks on the US or her allies. This alternative would be a poor strategy. The USAF should deliberately pursue robust cyber warfare capabilities that will preserve and expand the nation's future global strike abilities.

Bibliography

F.D. Kramer, et al. (eds.), *Cyberpower and National Security*. Washington, DC: Potomac Books, 2009.

Harald Sundmaeker, et al. (eds.), *Cluster of European Research Projects on the Internet of Things (CERP-IoT): Vision and Challenges for Realising the Internet of Things*. Brussels, 2010.

Air Force Doctrine Document (AFDD) 1. *Air Force Basic Doctrine, Organization, and Command*, 14 October 2011.

Aitel, Dave. "Three Cyber War Fallacies." Presentation. Usenix 2011, 9 August 2011. http://prezi.com/wdqab38lxr89/three-cyber-war-fallacies-usenix-2011/ (accessed on 14 January 2012).

Allen, Malcolm. "Social Engineering: A Means to Violate a Computer System." SANS Institute, 2007, available at: http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violate-computer-system_529 (accessed on 14 February 2012).

Berners-Lee, Tim. "Long Live the Web." *Scientific American*, Vol. 303, December 2010.

Berry, William, and Cheryl Loeb. "Breakthrough Air Force Capabilities Spawned by Basic Research." National Defense University, 2007.

Burkholder, Peter. "SSL Man-in-the-Middle Attacks." SANS Institute, 2002, available at: http://www.sans.org/reading_room/whitepapers/threats/ssl-man-in-the-middle-attacks_480 (accessed on 14 February 2012).

Chun, Wesley. "Using Federated Authentication via OpenID in Google App Engine." July 2010, http://code.google.com/appengine/articles/openid.html (accessed on 18 January 2012).

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Harper Collins, 2010.

Clarke, Roger. "The Digital Persona and its Application to Data Surveillance." *The Information Society*, June 1994, Vol. 10 Issue 2.

Clarke, Roger and Marcus Wigan. "You Are Where You've Been: The Privacy Implications of Location and Tracking Technologies." *Journal of Location Based Services*, December 2011, Vol. 5 Issue 3-4.

Crowcroft, Jon. "Future Internet Enervation." *ACM SIGCOMM Computer Communication Review*, June 2010, Vol. 40 Issue 3.

Franz, Timothy P. "IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way-Ahead for Network Warfare Forces." AFIT, March 2007.

Friedman, Thomas L. *The World is Flat: A Brief History of the Twenty-first Century*. 3rd ed. rev. New York: Picador, 2007.

Geis, John P., II, Christopher J. Kinnan, Ted Hailes, Harry A. Foster, and David Blanks. *Blue Horizons II: Future Capabilities and Technologies for the Air Force in 2030*. Maxwell Air Force Base: Air University Press, July 2009.

Hinchcliffe, Dion. "Twenty-two power laws of the emerging social economy." 5 October 2009, available at: http://www.zdnet.com/blog/hinchcliffe/twenty-two-power-laws-of-the-emerging-social-economy/961 (accessed 12 February 2012).

Hossfeld, Tobias and Phouc Tran-Gia. "Euroview 2010: Visions of Future Generation Networks." *ACM SIGCOMM Computer Communication Review*, July 2011, Vol. 41 Issue 3.

Ivancsy, Renata, and Sandor Juhasz. "Analysis of Web User Identification Methods." *World Academy of Science, Engineering and Technology*, 2007, Vol. 34, available at: www.waset.org/journals/waset/v34/v34-59.pdf (accessed 18 January 2012).

Jabbour, Kamal. “The Time has Come for the Bachelor of Science in Cyber Engineering.” *High Frontier*, August 2010, Vol. 6, Number 4.

Jabbour, Kamal and Sarah Muccio. “The Science of Mission Assurance.” *Journal of Strategic Security*, 2011, Vol. IV, Issue 2.

Kaku, Michio. *Physics of the Future: How Science Will Change Human Destiny and Our Daily Lives by the Year 2100.* New York: Doubleday, 2011.

Lessig, Lawrence. *Code version 2.0.* New York: Basic Books, 2006.

Liebowitz, S. J. and Stephen E. Margolis. “Network Externalities (Effects).” *The New Palgrave's Dictionary of Economics and the Law*, MacMillan, 1998.

Libicki, Martin. *Cyberdeterence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.

Libicki, Martin. “Pulling Punches in Cyberspace.” *Proceedings of a Workshop on Deterring Cyberattacks*, Washington, DC: The National Academies Press, 2010, 123-147, available at: http://www.nap.edu/catalog.php?record_id=12997 (accessed on 12 February 2012).

Lynn, William J. “Defending a New Domain: The Pentagon's Cyberstrategy.” *Foreign Affairs*, September/October 2010.

Mukhopadhyay, Somnath. “Global Diffusion of the Internet IX: Predicting Global Diffusion of the Internet: An Alternative to Diffusion Models.” *Communications of the Association for Information Systems*, Vol. 2006 Issue 17.

Nguyen, Vu, LiGuo Huang, and Barry Boehm. "An Analysis of Trends in Productivity and Cost Drivers over Years." 2010, available at: http://csse.usc.edu/csse/TECHRPTS/2010/usc-csse-2010-521/usc-csse-2010-521.pdf.

Nissenbaum, Helen F. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press, 2010.

Peterson, Matt. "Orkut Dissected: Social Networking in India & Brazil," 27 June 2011, http://www.aimclearblog.com/2011/06/27/orkut-dissected-social-networking-in-india-brazil/ (accessed 12 February 2012).

Phister, Paul W., Jr., Dan Fayette, and Emily Krzysiak . “CyberCraft: Concept Linking NCW Principles with the Cyber Domain in an Urban Operational Environment.” AFRL, 2007.

Rainie, Lee and Janna Anderson. *The Future of the Internet.* Pew Research Center, 2005.

Rainie, Lee and Janna Anderson. *The Future of the Internet II.* Pew Research Center, 2006.

Rainie, Lee and Janna Anderson. *The Future of the Internet III.* Pew Research Center, 2008.

Rainie, Lee and Janna Anderson. *The Future of the Internet IV.* Pew Research Center, 2010.

Rose, Charlie. “Silicon Valley Entrepreneur Discusses Internet’s Cyber Future.” *Charlie Rose Show* (MSNBC), 19 February 2009.

Rosin, Col Randolph. “To Kill a Mockingbird: The Deconstruction of Information Operations.” *Small Wars Journal*, 17 August 2009, http://smallwarsjournal.com/jrnl/art/the-deconstruction-of-information-operations (accessed 6 February 2012).

Schneier, Bruce. *Secrets & Lies: Digital Security in a Networked World.* Indianapolis, Indiana: Wiley Publishing, Inc., 2000.

Schwartz, Gen Norton A. chief of staff, US Air Force. Memorandum, “Invitation to Participate in the Blue Horizons Program for Academic Year 2012.” 19 May 2011.

Snir, Mark, William Gropp, and Peter Kogge. "Exascale Research: Preparing for the Post-Moore Era." 19 June 2011, available at: http://www.ideals.illinois.edu/bitstream/handle/2142/25468/Exascale%20Research.pdf (accessed 12 February 2012).

Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age.* (New York University Press, 2004).

Stevens, Michael. "Use of Trust Vectors to Support the CyberCraft Initiative." AFIT, 2007.

Sundararajan, Arun. "Local Network Effects and Complex Network Structure." *The B.E. Journal of Theoretical Economics*, 2007, Vol. 7, Iss. 1, Article 46.

Tucker, Patrick. "Building the Internet of the Future." *Futurist*, Jul/Aug 2009, Vol. 43 Issue 4.

US Securities and Exchange Commission. "Facebook SEC Form S-1 Filing." 1 February 2012, http://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287 (accessed: 4 February 2012).

USAF Chief Scientist. *Report on Technology Horizons: A Vision for Air Force Science and Technology, 2011-2030.* Volume 1, Washington, DC: 15 May 2010.

Wallace, Benjamin. "The Rise and Fall of Bitcoin." *Wired*, December 2011.

Walter, Chip. "Kryder's Law." *Scientific American*, 25 July 2005, available at: http://www.scientificamerican.com/article.cfm?id=kryders-law (accessed 12 February 2012).

Wicherski, Georg. "The Dangers of Social Networking." Kaspersky Lab SecureList Analysis, 19 April 2010, http://www.securelist.com/en/analysis/204792113/The_Dangers_of_Social_Networking (accessed 11 February 2012).

Zetter, Kim. "The Return of the Worm That Ate the Pentagon.," Wired, 9 December 2010, available on-line at: http://www.wired.com/dangerroom/2011/12/worm-pentagon/

Zittrain, Jonathan. *The Future of the Internet—and How to Stop It.* Yale University Press, 2008.

"Arbor Special Report: Worldwide Infrastructure Security Report VII, 2011." 7 February 2012, available at: http://arbornetworks.com/report (accessed 12 February 2012).

"Conference Report: Disruptive Civil Technologies, Six Technologies with Potential Impacts on US Interests out to 2025." 10 April 2008 Disruptive Civil Technologies Conference, sponsored by the US National Intelligence Council.

"PandaLabs Annual Report – 2011." 31 January 2012, available at: http://pandalabs.pandasecurity.com/pandalabs-annual-report-2011/ (accessed 12 February 2012).

"USAF Fact Sheet on EC-130J Commando Solo." http://www.af.mil/information/factsheets/factsheet.asp?id=182 (accessed: 6 February 2012).