AUGUST 2016

DIGITALLY-ENABLED WARFARE

The Capability-Vulnerability Paradox

Jacquelyn Schneider

Center for a New American Security

About the Author

JACQUELYN SCHNEIDER is a Ph.D. candidate in political science at George Washington University. Her research focuses on the intersection of national security, technology, and political psychology. Jacquelyn's work on cyber, intelligence, and unmanned technologies has appeared in *Journal of Conflict Resolution, Strategic Studies Quarterly*, online at War on the Rocks, and has been featured on Global Dispatches Podcast.

Before beginning her academic career, Jacquelyn spent six years as an Air Force officer in South Korea and Japan. She holds a B.A. in economics and political science from Columbia University and a M.A. in political science from Arizona State University.

Acknowledgements

The genesis of this project was a Cross-Domain Deterrence Conference organized by Dr. Erik Gartzke, Dr. Jon Lindsay, and Dr. Michael Nacht and funded through a Minerva grant. Thanks go out to the many individuals who have commented on earlier drafts, including Paul Scharre, Ben Fitzgerald, Loren Schulman, Richard Danzig, Dr. Charles Glaser, Dr. Caitlin Talmadge, Dr. Martha Finnemore, and scholars of the Institute for Security and Conflict Studies at George Washington University. I would also like to thank Maura McCarthy and Melody Cook for their role in the production, editing, and design of this report.

Cover Photo
Air Force Staff Sgt. Jerome Duhan prepares for a cyber readiness inspection at Altus Air Force Base, Oklahoma.
(Senior Airman Franklin R. Ramos /U.S. Air Force)

Over the last 20 years, digital technologies have revolutionized modern warfare. From network-centric warfare of the 1990s to Donald Rumsfeld's transformation to today's Third Offset, digital technologies have become the linchpin of U.S. weapons, tactics, and strategy. Soldiers on the battlefield coordinate air strikes using digital datalink and a tablet. Headquarters commanders, once reliant on radios to receive battle updates, watch digital feeds of streaming videos on common operating pictures populated by terabytes of near real time digital data. Cruise missiles and bombs receive satellite relays of digital navigation and targeting updates to destroy enemy targets day and night, in rain and snow, in foliage-covered jungles and dense urban centers. Digital data and the networks that store, process, and disseminate that data have made the U.S. military extraordinarily capable.

But these digital capabilities have also made the U.S. military extraordinarily vulnerable. A 2013 Defense Science Board Report warned, "the cyber threat is serious ... with present capabilities and technology it is not possible to defend with confidence against the most sophisticated cyber attacks."[1] The FY 2014 Annual Report from the DoD's Operational Test and Evaluation Director concluded, "the continued development of advanced cyber intrusion techniques makes it likely that determined cyber adversaries can acquire a foothold in most DoD networks, and could be in a position to degrade important DoD missions when and if they chose to."[2] Meanwhile, reports have surfaced of vulnerabilities within the defense industrial base[3] and next-generation weapons systems.[4]

As the DoD strives for greater digital capabilities, it becomes exponentially more effective on the battlefield and yet more vulnerable to pre-emptive attacks – both virtual and physical – on the digital networks and technologies that enable the U.S. military's modern lethality.

Together these capabilities and vulnerabilities create a dangerous dynamic for the United States. As the DoD strives for greater digital capabilities, it becomes exponentially more effective on the battlefield and yet more vulnerable to pre-emptive attacks – both virtual and physical – on the digital networks and technologies that enable the U.S. military's modern lethality. Further, as systems and tactics shift from digitally enhanced to digitally dependent, the United States may inadvertently place itself in a position to either take a debilitating first strike from adversaries or else strike first in order to preserve the digital capabilities necessary for modern warfare. This paradox of digital capability and vulnerability leads to an important consideration for U.S. policymakers: Do we go all in on digital warfare and accept the vulnerabilities in order to build the most capable military possible? Or do we sacrifice military capability in order to decrease the chance of inadvertent conflict?

Beyond Cyber Warfare: Digitally Independent, Digitally-Enabled, and Digitally-Dependent Warfare

The vast majority of discussion about digital advancements and war has focused on operations exclusively within the cyberspace domain, or "cyber warfare." However, what makes cyber warfare a potential game changer for modern conflict is the connection that states have built between digital capabilities and conventional warfare. These connections create lucrative cyber targets that impact conventional military effectiveness. It is therefore important to understand not only a state's (or non-state's) cyber capabilities, but also its use of digital technologies to conduct conventional conflict within the air, sea, land, and space domains. For some states, digital capabilities play only a small role in their overall strategy, while others' digital capabilities are linchpins in their conventional warfighting strategies. Whether a state is only marginally reliant on digital technologies, completely independent of these technologies, or completely dependent on them has a significant impact on both crisis dynamics and conventional military capabilities. Three categories of digital dependency illustrate how the spectrum of digital reliance impacts conflict: digitally-independent, digitally-enabled, and digitally-dependent states.

Digitally-Independent States

Digitally-independent states use almost no digital technologies to conduct conventional warfighting. This means their weapons generally are not linked to larger networks and can conduct only basic line-of-sight targeting functions. Communications are limited to fixed cable, analog satellite relays, and radio/high frequency transmissions. For digitally-independent militaries, command and control over the horizon is significantly limited, mobile operations are difficult, if not impossible, to execute, and large data transfers are either very slow or impossible. Intelligence is primarily human, manned aircraft photography, or non-cyber signals intelligence. States that are digitally independent have trouble conducting coordinated, decentralized warfare and have limited ability to respond in near real time to adversary changes or conduct dynamic precision targeting. These states are, however, less vulnerable to cyber attacks. Their reliance on less sophisticated and less diffuse networks leaves very few useful cyber targets and means that attacks on digital infrastructures are less likely to affect overall combat effectiveness.

Very few states today are completely digitally independent. However, there are states that – with limited military budgets, few larger nations willing to support them, and perhaps a largely domestic security focus – are still reliant on Cold War-era analog technologies. These are, for example, states like Cuba or Zimbabwe. To date, digital independence has been less a conscious strategy for states to mitigate vulnerabilities and more a default condition created because of lack of resources or security needs.

Digitally-Enabled States

Digitally-enabled states use digital technologies to enhance operations, but are not fully dependent on that digital technology to conduct military campaigns. For example, a digitally-enabled state may use digital datalinks to convey off-site targeting information to a radar facility, but would still be able to use that radar facility's organic targeting capability if the off-site information was no longer available. Digitally-enabled states use technologies like digital communications and cyber intelligence to increase their overall situational awareness and conduct decentralized operations. They are therefore able to conduct network-centric operations. However, they may still have in place analog or hard-copy processes that impact the ability to maximize network-centric warfare. This ability to operate without digital capabilities may be a deliberate choice by the state to build resiliency and retain the capability to conduct platform-centric operations. It also may be an unintentional consequence of limited resources or a limited ability to update analog capabilities to more effective digital capabilities. The vast majority of states are within the spectrum of digitally-enabled nations, and range from highly proficient militaries such as Japan and South Korea to less proficient but emerging digital militaries like Iran and Brazil.

It is therefore important to understand not only a state's (or non-state's) cyber capabilities, but also its use of digital technologies to conduct conventional conflict within the air, sea, land, and space domains.

Digitally-Dependent States

Digitally-dependent states rely on digital technologies to conduct conventional warfare. These states build campaigns based on the ability to utilize digital technologies to conduct network-centric operations. Digitally- dependent states optimize decisionmaking speed and situational awareness with datalinks and virtual computing but do not retain capabilities to conduct non-digitized operations, and therefore have limited ability to utilize platform-centric campaigns in which weapon systems operate off-network, independent of centralized command and control or communication support. For example, digitally-dependent states maximize efficiencies by off-boarding intelligence, targeting, and navigation from platforms (for example, the aircraft carrier) to larger databases of information centrally processed and stored in data fusion centers. Digitally-dependent states build weapons that are optimized with near real time information and digital processing, but also require digital updating in order to be effective. Few, if any, states are completely digitally dependent yet, but many modern militaries – such as the United States, the United Kingdom, and increasingly China – are seeking digital capabilities that may move them closer to the digital dependency spectrum.

Few, if any, states are completely digitally dependent yet, but many modern militaries – such as the United States, the United Kingdom, and increasingly China – are seeking digital capabilities that may move them closer to the digital dependency spectrum.

A useful way to conceptualize the difference between digitally-independent, digitally-enabled, and digitally-dependent warfare is to use the analogy of the evolution of cars. For instance, a 1970s sedan lacks automatic options or digital add-ons. Windows have to be rolled down by hand; gauges and engine warnings are limited to coarse measurements. By the ’90s, that same sedan has automatic locks and windows and maybe even an unsophisticated computer system. And 20 years later, that same sedan is run by an inboard computer and everything from locks to ignitions is remotely controlled. Further, the current sedan offers navigation and even onboard Wi-Fi. As with our digitally-independent nations, the 1970s sedan is not nearly as advanced as the sedan of the ’90s or current model, but it also isn’t prone to costly repairs of the updated features found in the ’90s sedan. And similarly, the 1990s sedan lacks navigation or updated computer systems, but is still drivable if its primitive onboard computer system fails. In the sedan of today, the digital systems undergird the entire car, making them the most responsive, powerful, and efficient ever. However, for these sedans (unlike their vehicular ancestors), a digital display is not an optional feature but a costly and necessary repair. Further, these networked and navigated sedans of today also are vulnerable to remote access and cyber attacks.[5] For example, Fiat and Chrysler recalled millions of cars after hackers remotely took control of a Jeep Cherokee and drove the digitally tricked-out car into a ditch.

The Capability/ Vulnerability Paradox and Digital Warfare

What does this spectrum of digital capabilities mean for modern warfare? First, digitally-enabled warfare allows states to project power over great distances, at condensed time ranges, and with great precision and lethality.[6] But these highly effective digitized capabilities also introduce new vulnerabilities to states as they become more dependent on cyber in order to operate tactically, operationally, and strategically. Therefore, digital capabilities produce a trade-off for states in which they must determine at what point they are effective enough to achieve military objectives but also are able to mitigate network vulnerabilities from an adversary's first-move attack. The paradox of cyber for modern warfare is that states may become extremely effective – to the point of dominance – if they are able to create a digitally-enabled military. However, as states become more dominant and move from digital enablement to digital dependence, they also become more reliant on networks to conduct operations, thus making them vulnerable to first strikes from opposing adversaries (even adversaries that may not be able to compete in a full digitally-enabled conflict). This creates an even stranger paradox so that as states move from digitally enabled to digitally dependent, a more powerful state may have to take a first-move attack, despite being overwhelmingly more capable than their adversary, to ensure an adversary is unable to exploit network or technology vulnerabilities.

To better understand this paradox, take the case of one weapon system: an analog fire control radar on a surface to air missile (SAM) versus a digitally upgraded fire control radar on the same system. The analog radar requires significant operator training; the scope is difficult to interpret, the radar is limited in its ability to process target location, and higher headquarters can only pass a few instructions or targets from off-board sources. The digital radar, on the other hand, requires limited operator training and provides displays that are easy to interpret. As Dr. Carlo Kopp of the think tank Air Power Australia explains, "the demands for proficiency and technical understanding of operation by crews seen in early Cold War SAM systems no longer exist – operators have sophisticated LCD panel displays with synthetic presentation."[7]

Furthermore, the digital system integrates targets passed from off-board platforms and higher headquarters, enabling the same radar to prosecute more targets with greater fidelity. Because the digital system can process targets with greater speed and at a greater capacity, it is also able to automatically counter electronic countermeasures such as jamming or spoofing. Therefore, due to the capacities imbued by these digital upgrades, the same SAM – with digital upgrades – provides greater situational awareness and higher probability of kill. For example, the digitally upgraded SA-3, otherwise known as the Pechora 2M, has a greater range of detection, higher number of targets it can track, and an overall higher probability of kill than the analog SA-3 (advertised .5 probability of kill with the analog system and .72-.99 probability of kill with the digital system).[8]

However, the digital system also is vulnerable to network attack, whereas the analog system – because of its lack of connectivity to the network and reliance on hardware over software – is generally resilient. The networks that the digital system connects to (for example, the network that connects the radar to higher headquarters), the software that the system uses to process and display information, and the hardware (which often must be outsourced) that the system uses in its computers, servers, and modems are potential targets for enemy attack.[9] There have been reports not only of the potential of the vulnerabilities,[10] but of actual incidents in which these air defense networks have been attacked by a series of kinetic and non-kinetic means. In 2007, Israeli aircraft were able to penetrate Syrian airspace with no reaction from the fairly competent Syrian air defenses. Later reports indicated that

The paradox of cyber for modern warfare is that states may become extremely effective – to the point of dominance – if they are able to create a digitally-enabled military … as states become more dominant and move from digital enablement to digital dependence, they also become more reliant on networks to conduct operations, thus making them vulnerable to first strikes from opposing adversaries.

the Israelis had perhaps used a cyber attack on Syria's upgraded air defense technologies to shut down the systems immediately prior to the attack.[11] Further, because upgraded radar systems are highly automated and don't require the technician to understand the basics of the system in order to operate, technicians who train on and operate digital systems potentially lose the ability to manually identify and then override any deception or manipulation attack on the system. Therefore, the digitally upgraded fire control radar significantly increases the capability of the missile system, but also introduces new and potentially debilitating vulnerabilities.

This is one example of the capability/vulnerability paradox, but it is part of a larger pattern of weapons developments in which digitally-enabled platforms are both more capable and more vulnerable than their non-cyber compatriots. And because of this paradox, digitally-enabled/dependent states can be conventionally dominant and yet find themselves in inadvertent conflict.

The dynamic of extreme capability and critical vulnerabilities creates two incentives for first strikes. First, in a potential crisis scenario, a state that is less capable has an incentive to strike first at a more capable/digitally-dependent state's networks because the less capable state knows it cannot survive unless it is able to cripple the digitally-enabled state's advantage. Second, as a more capable digitally-enabled state moves closer to digital dependency, it is also incentivized to make a first move because it cannot effectively operate without access to networks and digital inputs and is aware of its vulnerability. The more digitally-capable state must use its conventional dominance to preemptively destroy the adversary's first strike weaponry. Therefore, in order to maximize their chances of military victory, both the more powerful and the less powerful state have an incentive to move first in a crisis.

Is this paradox unique to cyber or cyber-enabled capabilities? Likely not – but this trade-off is different than other tit-for-tat cycles of weapon development, partly because of the unique qualities of cyberspace. First, the current consensus is that there is an offensive advantage in cyberspace.[12] Therefore, as we create new targets in cyberspace with the expansion of digital weaponry, we do not proportionally increase our ability to defend against cyber attacks. This may change in the future with technological innovations, but in its current state the offensive advantage in cyber makes it impossible to be both digitally dependent and only mildly vulnerable. Cyber is further unique from other weapons because actions in cyberspace can be taken quickly, virtually, and remotely, to a scale not possible with physical weapons. These characteristics may inadvertently increase the potential for conflict escalation. For instance, the future development of network defenses with automated hack-backs[13] could create virtual tripwires that would inherently increase the danger of the cyber capability/vulnerability paradox.

Cyber as an Infrastructure

The cyber capability/vulnerability paradox is also different than other types of weapons development because the cause of this paradox is not a particular platform or weapon capability, but the way in which cyber creates an infrastructure of capabilities and vulnerabilities that connects to a family of weapons and platforms. In that sense, the advancements that cyber technologies bring to modern conflict may be better likened to the impact of the development of roads, railroads, or combustion engines than to the rifle, the tank, or the aircraft carrier. Digital technologies are integrated into every domain, across weapon systems, and across all levels of warfare. Because of their ubiquitous nature and infrastructural characteristics, the capabilities and the vulnerabilities they imbue are exponential as opposed to strictly additive.

In examining analogies within infrastructure development and conflict, a historical pattern of capabilities and vulnerabilities that illustrate the logic of the capability/

	HIGH VULNERABILITY	LOW VULNERABILITY
High Capability	Digitally-dependent Most capable Most likely for inadvertent conflict	Not possible with current technology
Medium Capability	Digitally-enabled	Digitally-enabled Most stable Best case scenario
Low Capability	Digitally-incompetent	Digitally-independent Least likely to win conflict Least likely for inadvertent conflict

vulnerability paradox emerges. Take, for example, the combustion engine. Internal combustion engines opened up remarkable opportunities for weapons development – from tanks to aircraft to ships, combustion engines made nations more effective on the battlefield. But it also made them more dependent on oil and therefore vulnerable to disruptions in the oil supply chain. This paradox created (and to some extent continues to create) an international scenario in which states without access to oil, but heavily reliant on oil to fuel their military, were induced to seek first-move attacks in order to fend off major vulnerabilities to their oil supply. The classic example is Japan in World War II, in which a U.S. oil embargo that threatened to ground the Japanese navy played heavily in the Japanese decision to pre-emptively attack Pearl Harbor.

Capability/Vulnerability Paradox Beyond the Military

Recent events demonstrate the relevance of this paradox even beyond the military dimension. In one day, on July 8, 2015, 1,200 United Airlines flights were grounded due to a router malfunction,[14] the New York Stock Exchange ceased trading for four hours due to a software configuration issue,[15] and the *Wall Street Journal* website malfunctioned after a server overload.[16] And while none of these examples include malicious attack, they demonstrate the exponential nature of the vulnerabilities of digital dependency. As Richard Danzig points out, "digital technologies … are a security paradox: even as they grant unprecedented powers, they also make users less secure … their concentration of data and manipulative power vastly improves the efficiency and scale of operations, but this concentration in turn exponentially increases the amount that can be stolen or subverted by a successful attack. The complexity of their hardware and software creates great capability, but this complexity spawns vulnerabilities and lowers the visibility of intrusions … in sum, cyber systems nourish us, but at the same time they weaken and poison us."[17] Additionally, these digital technologies – the Internet of Things – that speak to each other, seamlessly derive data, share information, and communicate with users and other technologies also create new targets for cyber attacks and new windows through which systems can be hacked. Whether it is digitally-enabled home locks, remote sprinklers, or fitness trackers, these civilian examples of digital vulnerabilities and capabilities demonstrate the dangerous nature of the vulnerabilities that emerge from extreme digital capabilities.

U.S. Conventional Operations: Digitally-Enabled Moving Toward Dependence?

According to the capability/vulnerability paradox, as a state moves toward digital dependence, there is a dangerous incentive for both adversaries and the more capable digital-dependent state to take first-move strikes. Therefore, digital dependencies can make crises less stable and conflict more likely. Where is the U.S. military on the digital spectrum and how might that impact future crises?

The United States' relationship with digitally-enabled warfare has evolved since its inception in the 1990s. From rudimentary email and a handful of digitally-upgraded weapons to a fleet of unmanned aircraft, intelligence processing facilities (distributed common ground systems), remote operations video enhanced receivers (ROVER), and operations command centers connected by sophisticated satellite and fiber networks, the U.S. military has successfully built a digitally-enabled force able to provide near real time situational awareness, precision targeting, and joint integration across and within chains of command.

But these weapon systems increasingly are moving from an enabled force to one that is dependent on network targeting information, digital satellite communication to GPS networks, and digital command operating pictures/blue force trackers to execute the multi-line of approach, highly complex operations of 21st-century U.S. military campaigns. As the 2012 *Defense Strategic Guidance* asserted, "modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space. Cyber enables U.S. success and yet makes network-dependent operations highly vulnerable to cross-domain cyber threats."[18] Despite this acknowledgement of the vulnerabilities inherent in a digitally dependent strategy, the Third Offset strategy advanced by DoD appears to go all in on the extreme capabilities of a digitally-dependent military, investing in increasingly automated systems, big data, and information sharing/optimized weaponry.[19]

Indeed, as we appraise the weapon systems and operations that the United States has developed over the last 20 years, we see an inventory of technologies and a set of human skills that are highly effective on the battlefield and yet also highly vulnerable to network attack. Two examples of U.S. weapons technologies and tactics exemplify this paradox – both of which comprise major elements of the DoD budget, were identified in the 2014 *Quadrennial Defense Review* as key technologies, play

Air Force personnel analyze intelligence, surveillance, and reconnaissance data through the Air Force Distributed Common Ground System. (U.S. Air Force)

pivotal roles in the joint operational access concept, and epitomize the Third Offset: the distributed common ground system (DCGS) and the F-35. The vulnerabilities inherent in these platforms, which are problematic in their own right, are outlined in this section. However, it is the systematic acquisition and development of similar digitally-dependent technologies that moves the United States toward digital dependency and makes the U.S. military highly capable and highly vulnerable.

The Air Force DCGS, also known as the AN/GSQ-272 Sentinel, serves as the control, processing, and exploitation center for intelligence data across a wide variety of sources – whether that be aerial overhead imagery platforms, signals intelligence aircraft, air battle management aircraft, etc.[20] According to the U.S. Air Force, each of the 12 operational DCGS facilities boast "more than 50 ISR sorties exploited, over 1,200 hours of motion imagery reviewed, approximately 3,000 signals intelligence (SIGINT) reports produced, 1,250 still images exploited and 20 terabytes of data managed daily."[21] Before digital technologies, intelligence platforms conducted sorties, flew home, dropped off their intelligence – whether that be photos or electronic recordings – sent the highly technical intelligence back to agencies that specialized in that particular exploitation, and then disseminated information through cables or hard copies of the data. With the DCGS, information can be received, processed, analyzed, and disseminated in the same place and near real time. This provides revolutionary threat awareness – the backbone of the blinding operations, attacks in depth, and decentralized operations of cyber-enabled warfare.

But as critical processing centers for the U.S. military's operations, they also are fantastic targets for attack, whether these attacks be cyber or kinetic. Without access to send information to these centers, aerial platforms would have to land at their base and upload vast quantities of information through portals not optimized for raw intelligence or intelligence of great magnitude. Intelligence would no longer be near real time and operations centers once again would have to rely on time-delayed intelligence and, potently, be limited to raw aerial intelligence that was collected near the operating center. Further, because these systems are highly complex with a myriad of different inputs, processors, and software, they walk a delicate line of extreme capability and inoperability. In a review of a similar platform, the DCGS-Army, the Army Test and

Evaluation Command found that the extremely complicated nature of the highly networked DCGS-Army led to the platform being too complex, unreliable, and ultimately "not survivable."[22]

The F-35 presents an ideal example of the capability/vulnerability paradox of digitally-enabled warfare. The F-35 boasts stealth capability, integrated electronic attack, digital displays, information sharing, and unprecedented sensor fusion.[23] The F-35 is an airpower force multiplier – the "quarterback" of air operations, utilizing its advanced network and sensor suite to distribute information and target allocation across the air picture.[24] Instead of relying on the platform's sensors to conduct operations, the F-35 can take information from its own advanced sensors and others from off-board data fusion centers. As U.S. Navy test pilot Commander Burke stated in an interview about the platform, "In the future, it may not matter where the weapon comes from. I may pass the data along, or I may fire a weapon and it may come from somewhere else. That is where we are heading."[25] Near real time integration of off-board and onboard sensors facilitates decentralized operations, multiple lines of effort, and effective/flexible allocation of targets, even while in flight.

Tech. Sgt. Brandon Sullivan digitally connects technical data to an F-35 trainer as part of a weapons familiarization course. (Maj. Karen Roganov /U.S. Air Force)

But this integration is in itself a major vulnerability for the F-35 because it provides key cyber terrain that must be held in order to perform its mission. And this mission – the ability to share information and build awareness in the air – has become central to air doctrine in modern U.S. tactics. General Michael Hostage, previously the head of Air Combat Command, explains, "The ability of the planes to work with each other over a secure distributed battlespace is the essential foundation from which the air combat cloud can be built. And the advantage of the F-35 is the nature of the global fleet. Allied and American F-35s, whether USAF, USN, or USMC, can talk with one another and set up the distributed operational system. Such a development can allow for significant innovation in shaping the air combat cloud for distributed operations in support of the Joint Force Commander."[26] This is part of a larger plan within the joint operational access concept to provide situational awareness across the Pacific through the networking of sensors and platforms. Therefore, the F-35 vulnerabilities tied to in-flight data dissemination do not just have the potential to limit the platform's operational effectiveness, but have the potential to threaten the entire operational concept: "The strategic thrust of integrating modern systems is to create a grid that can operate in an area as a seamless whole, able to strike or defend simultaneously. This is enabled by the evolution of C5ISR, and it is why ... 5th generation aircraft are not merely replacements for existing tactical systems, but a whole new approach to integrating defense and offense."[27]

Even the maintenance and support suite of the F-35, the Automatic Logistics Information System (ALIS), requires network connectivity in order to manage F-35 operations. And that connectivity is potentially vulnerable. The system tracks F-35s, both in flight and on the ground, providing information about the health of the aircraft, where they are located, and what needs to be done to maintain the aircraft. These are functions that, in other platforms, are tracked by an onerous system of manual maintenance logs and records. ALIS provides revolutionary support to keep the F-35s healthy and operational. However, when a U.S. Navy red team of cyber experts attempted to infiltrate the system, not only were they able to hack in, they were able to do so unseen.[28] Hacks into the maintenance system, without manual backup, could ground a fleet of F-35s.

The DCGS and the F-35 are just two examples of the move that the U.S. military is taking toward digital

dependency. These systems are not uniquely vulnerable. Rather, they are emblematic of the increased vulnerability that comes with increased digital dependency, a tradeoff that is seen in many other programs. The United States also continues to invest heavily in unmanned aircraft and precision-guided technology, all while developing campaigns that rely on cyberspace dominance to execute operations. At the same time, both U.S. adversaries and elements of the U.S. military recognize the reliance and vulnerability of U.S. conventional dominance on digital technologies. As the 2015 *Chinese Science of Military Strategy* proclaims, "victory in war first starts from victory in cyberspace; whoever seizes the initiative in cyberspace will win the initiative in war."[29]

Conclusions and The Way Forward

What does this mean for U.S. military power? In most situations, and at most times, the digitally-enabled and increasingly dependent force that the United States has constructed will provide a strong deterrent and a capable tool of coercion against adversaries. However, if the United States continues to build weapons and campaigns that move toward digital dependency, then it may find itself in a tenuous situation where it must either strike first or be prepared to function without much of its digital capability.

What then should the United States do? First, the U.S. military needs to focus greater attention, both within the acquisition process and during training and tactics development, on digital resiliency. This resiliency could include acquiring technologies with both digital and manual capabilities or developing systems with both automated and man-in-the-loop modes of performance. But resiliency also will likely require increased manned training and tactical proficiency for back-up manual procedures and off-net (or off-datalink) operations. And, perhaps most difficult, this requires building campaigns that are not dependent on digital capability. The most capable and least dangerous future military is one in which digital technologies enhance capabilities but are not uniquely critical vulnerabilities in campaign strategies.

The U.S. military needs to focus greater attention, both within the acquisition process and during training and tactics development, on digital resiliency.

This is not particularly new or revolutionary, but it does require potentially sacrificing some level of digital effectiveness in order to mitigate vulnerabilities, making this a difficult trade-off decision both politically and militarily. Retaining legacy systems and hard-copy processes is expensive and time-consuming. Building new technologies that can operate without datalinks or top-of-the-line computing capability may seem like we are needlessly handcuffing ourselves. Meanwhile, designing operational campaigns that limit critical digital dependencies may mean that we take away valuable training time from honing digital weapon prowess to focus on time-consuming and less effective combat skills. However, sacrificing some level of digital capability may paradoxically make the United States more secure. For instance, a recent U.S. Government Accountability Office evaluation of the U.S. nuclear program called out the command and control technology, which relies on floppy disks and assembly language code, as being inefficient and almost obsolete.[30] It called for technological upgrades, but paradoxically the aging technology of the nuclear command and control system makes the United States less vulnerable to cyber attacks on our nuclear weapons infrastructure.

Finally, the vast majority of discussion and policy momentum about the role of digital technologies in future conflict has been focused on cyber weapons system or defense. However, this study suggests that we must do a better job of understanding how cyber enables conventional weapons, operation, and doctrine. Solving this digital paradox may be difficult, but recognizing that it exists will be the first step toward mitigating risks and generating institutions, tactics, weapons, and operations that long-term U.S. national security objectives.

Endnotes

1. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Resilient Military Systems and the Advanced Cyber Threat*, January 2013, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

2. DoD Operational Test and Evaluation, *FY2014 Annual Report*, http://www.dote.osd.mil/pub/reports/fy2014/pdf/other/2014DOTEAnnualReport.pdf.

3. Sean Lyngaas, "Pentagon Warns Contractors of Juniper Vulnerabilities," *FCW Magazine*, January 6, 2016, https://fcw.com/articles/2016/01/06/dss-juniper-guidance.aspx.

4. Marina Malenic, "DoD chief tester warns on F-35 cyber, software issues," *IHS Jane's*, January 26, 2016, http://www.janes.com/article/57454/dod-chief-tester-warns-on-f-35-cyber-software-issues.

5. Aaron Kessler, "Fiat Chrysler Issues Recall Over Hacking," *The New York Times,* July 24, 2015, http://www.nytimes.com/2015/07/25/business/fiat-chrysler-recalls-1-4-million-vehicles-to-fix-hacking-issue.html; Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me In It," *Wired*, July 21, 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; Andy Greenberg, "How Hackable is your Car? Consult this Handy Chart," *Wired*, August 6, 2014, http://www.wired.com/2014/08/car-hacking-chart/.

6. Erik Dahl, "Network Centric Warfare and Operational Art," *Defence Studies* 2/1(Spring 2002): 17.

7. Carlo Kopp, "Surface to Air Missile Effectiveness in Past Conflicts," *Air Power Australia,* October 2010, http://www.ausairpower.net/APA-SAM-Effectiveness.html.

8. Carlo Kopp, "Legacy Air Defence System Upgrades," *Air Power Australia*, June 2009, http://www.ausairpower.net/APA-Legacy-SAM-Upgrades.html.

9. Chandler Atwood and Jeffrey White, "Syrian Air Defense Capabilities and the Threat to Potential U.S. Air Operations," *The Washington Institute*, May 23, 2014, http://www.washingtoninstitute.org/policy-analysis/view/syrian-air-defense-capabilities-and-the-threat-to-potential-u.s.-air-operations.htm.

10. Jim Michaels, "U.S. could use cyber attack on Syrian air defenses," *USA Today*, May 16, 2013, http://www.usatoday.com/story/news/world/2013/05/16/syria-attack-pentagon-air-force-military/2166439/.

11. David Eshel, "Cyber Attack Deploys in Israeli Forces," September 16, 2010, https://www.mail-archive.com/infowarrior@attrition.org/msg06295.html; John Markoff, "A Silent Attack, but not a Subtle One," *The New York Times*, September 26, 2010, http://www.nytimes.com/2010/09/27/technology/27virus.html?hp&_r=0; Lewis Page, "Israeli sky-hack switched off Syrian radars countrywide," *The Register*, November 22, 2007, http://www.theregister.co.uk/2007/11/22/israel_air_raid_syria_hack_network_vuln_intrusion/.

12. Ilai Saltzman. "Cyber Posturing and the Offense-Defense Balance." *Contemporary Security Policy* 34, No.1 (2013), 40-63; Keir Leiber, "The Offense-Defense Balance and Cyber Warfare," in *Cyber Analogies,* eds. Emily Goldman and John Arquilla (Monterey: Naval Postgraduate School, 2014); Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," *Strategic Analysis* 34, no.1 (2010), 62–73; Richard Clarke and Robert Knake, *Cyber War* (New York: Harper Collins, 2011); William Lynn, "Defending a New Domain-The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no.5 (2010); 97-108; Richard Clarke, "War from Cyberspace." *National Interest* no.104 (2009): 31-36; Dorothy Denning, "Barriers to Entry: Are They Lower for Cyber Warfare?" *IO Journal* (2009): 6-10; Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38, no.2 (2013): 7-40; Patrick Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy*.

13. Hannah Kuchler, "Cyber Insecurity: Hacking Back," *Financial Times,* July 27, 2015, http://www.ft.com/cms/s/2/c75a0196-2ed6-11e5-8873-775ba7c2ea3d.html#axzz4FEPNnC8z.

14. Michael Sasso and Lauren Thomas, "United Computer Failure Spanned Multiple Systems as Woes Persist," *Bloomberg*. July 8, 2015, http://www.bloomberg.com/news/articles/2015-07-08/united-computer-failure-spanned-multiple-systems-as-woes-persist.

15. Nathaniel Popper, "The Stock Market Bell Rings, Computers Fail, Wall Street Cringes," *The New York Times*, July 8, 2015, http://www.nytimes.com/2015/07/09/business/dealbook/new-york-stock-exchange-suspends-trading.html?_r=0.

16. "Tech fail! Explaining today's 3 big computer errors," *CNN Money*, July 8, 2015, http://money.cnn.com/2015/07/08/technology/united-nyse-wsj-down/.

17. Richard Danzig, "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies," (*Center for New American Security*, July 2014), 5, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_PoisonedFruit_Danzig_0.pdf.

18. U.S. Department of Defense, *Sustaining US Global Leadership: Priorities for 21st Century Defense,* 2012, 6, http://www.defense.gov/news/defense_strategic_guidance.pdf.

19. Aaron Mehta, "Work Outlines Key Steps in Third Off-

set Tech Development," *Defense News,* December 14, 2015, http://www.defensenews.com/story/defense/innovation/2015/12/14/work-third-offset-tech-development-pentagon-russia/77283732/.

20. Raytheon, "Distributed Common Ground System (DCGS)," http://www.raytheon.com/capabilities/products/dcgs/.

21. U.S. Air Force, "Air Force Distributed Common Ground System," October 2015, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104525/air-force-distributed-common-ground-system.aspx.

22. Greg Slabodkin, "Distributed common ground system comes under fire," Defensesystems.com, October 1, 2012, http://defensesystems.com/articles/2012/10/01/defense-it-2-distributed-common-ground-system.aspx.

23. Lockheed Martin, "F-35 Lightning," https://www.f35.com/about.

24. Ibid.

25. As cited in Robert Ackerman, "F-35 Offers Dream Capability for Pilots Who Have Flown it," *Signal Online*, February 11, 2014, http://www.afcea.org/content/?q=node/12336.

26. Robbin Laird, "Why Air Force Needs Lots of F-35s: Gen. Hostage on the 'Combat Cloud,'" *Breakingdefense.com*, January 10, 2013, http://breakingdefense.com/2013/01/why-the-air-force-needs-a-lot-of-f-35s-gen-hostage-on-the-com/

27. Robbin Laird, "Game Changer: The F-35 and the Pacific," *The Diplomat*, April 25, 2013, http://thediplomat.com/2013/04/game-changer-the-f-35-and-the-pacific/1/.

28. Andrea Shalal-Esa, "Insight: Lockheed's F-35 logistics system revolutionary but risky," Reuters, November 16, 2012, http://www.reuters.com/article/2012/11/16/us-lockheed-fighter-logistics-idUSBRE8AF09L20121116.

29. Elsa Kania, "The Latest Indication of the PLA's Network Warfare Strategy," *China Brief* 15(24): December 21, 2015, http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=44925&no_cache=1#.VvqbAUvCSIx.

30. United States Government Accountability Office, "Federal Agencies Need to Address Aging Legacy Systems," May 2016, http://www.gao.gov/assets/680/677436.pdf.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

1152 15th Street, NW Suite 950 Washington, DC 20005

t. 202.457.9400 | f. 202.457.9401 | info@cnas.org | cnas.org

Bold. Innovative. Bipartisan.