DEFENSE DOSSIER

SEPTEMBER 2013 ISSUE 8

American Foreign Policy Council

DEFENSE DOSSIER

September 2013 ISSUE 8

American Foreign Policy Council

FROM THE EDITORS

Welcome to the September 2013 edition of the Defense Dossier, the e-journal of the American Foreign Policy Council (AFPC). In this issue, we focus on the intersection of high technology and national security, and on the potential impediments that exist for U.S. operations in the global commons.

Modern day technology has brought about great advancements in military affairs and intelligence collection. In the process, however, it has also raised new and pressing questions about privacy, security and morality among the general public. The recent leaks from NSA whistleblower Edward Snowden have generated a spirited debate on the tensions between privacy and national security. Similarly, the prevalence of drones—and the potential to remove humans from the loop during conflict—have raised questions about the legality and morality of autonomous weapons systems on the battlefield. In the global commons, meanwhile, there are new vulnerabilities in space, limitations to energy access at sea, and potential for the degradation of U.S. air dominance in future conflicts.

This issue of the Dossier explores each of these topics and their respective impacts on U.S. national security. We hope these articles help to enhance the popular understanding of these complex issues.

Sincerely,

Ilan Berman
Chief Editor

Richard Harrison
Managing Editor

THE TENSION BETWEEN PRIVACY AND CYBER SECURITY

MARY DEROSA

On July 24, 2013, the House of Representatives voted 217 to 205 to reject a proposed amendment to the Defense appropriation bill that would have defunded the National Security Agency's (NSA's) telephony metadata program due to privacy concerns. This was a surprisingly close call for a program that the Obama administration and many in Congress consider a valuable contributor of foreign intelligence related to terrorist threats. The vote was only one example of the significant impact of the leaks by Edward Snowden, a former NSA contractor, of highly-sensitive materials relating to NSA operations.

We are in a period of heightened concern about privacy and national security. Although the public's focus so far has been on NSA surveillance operations, government efforts to address cyber security are sure to be affected. Indeed, soon after Snowden's disclosures, 38 civil society organizations and technology companies sent a letter to senators involved in negotiating cyber security legislation. The letter refers to "The newly disclosed NSA programs," which the authors say "clearly illustrate that the government will interpret any surveillance laws aggressively," and calls for a variety of privacy protections in any potential cyber legislation. According to the Center for Democracy and Technology, the message of the letter is, "we're watching."

SPEAKING DIFFERENT LANGUAGES

There has always been a disconnect between the national security and privacy communities. They speak fundamentally different languages.

Distrust of a powerful government is a basic element of the privacy community's worldview. The Federal Government has often earned that distrust by using U.S. citizens' private information to violate their civil liberties, usually in the name of national security. Therefore, privacy advocates believe the Executive Branch as a whole should never entirely be trusted to handle private data. The policy solution to these concerns has been to control collection of private data—keeping that data out of government hands unless necessary. When collection is necessary, they believe, it should be strictly limited and overseen by other branches of government. Internal Executive Branch controls on use of private data are met with distrust. Claims by government officials of good intentions or great need have little impact.

Those in the national security community who collect and use this information often find this attitude puzzling at best, and deeply offensive at worst. Their reaction to concerns that they would use information to spy on Americans or violate their civil liberties is, "why would I want to do that?" Their goal is to find and address grave national security threats –to protect the American public, not threaten it. They seek the information only because they believe it will help them to be effective. The vastly greater availability of communications data that we see now is, to them, an opportunity for more powerful protection, not for abuse. Moreover, those who carry out the surveillance programs that are now so controversial believe they operate under significant, sometimes even counter-productive, oversight. These operators see level after level of oversight of their actions—from Congress, the Foreign Intelligence Surveillance Court (FISC), the Justice Department, the office of the Director of National Intelligence, and the NSA's Inspector General and lawyers. In their view more constraints would only reduce their ability to carry out their responsibilities.

What makes this disconnect immeasurably worse is that

Mary DeRosa *is a Distinguished Visitor from Practice at the Georgetown Law School, where her focus is national security law. She has served as Deputy Counsel to the President and National Security Council Legal Adviser in the Obama administration, and earlier as Chief Counsel for National Security for the Senate Judiciary Committee and as a lawyer on the staffs of the National Security Council and Department of Defense.*

so often the details of collection, constraints, and oversight are secret. Secrets breed distrust. The NSA—an extremely secretive agency with powerful tools—is a target of particular suspicion in the privacy community.

It is an additional complication that privacy has never fit naturally into national security policymaking. Ideally, security and privacy are reinforcing values and both can be optimized. In practice, though, the privacy voice within the Executive Branch—and there are many committed people who do an excellent job of articulating privacy issues—almost always seems to make the job harder. Moreover, there is a tension in the role of the privacy advocate in the government between being an independent overseer and being a part of the team. All too often, the result is that the privacy perspective is not incorporated effectively in the very early stages of developing technology, programs, or policy, when it could be the most helpful.

PRIVACY AND CYBER SECURITY

All of these issues can affect cyber security discussions. But there has been a somewhat different approach to privacy and cyber policy over the past few years. The Obama administration has done a good job of incorporating privacy protections into its cyber security efforts, and there has been a great deal of public discussion of privacy issues related to cyber.

Cyber security efforts that have raised particular privacy attention and concern include the Einstein intrusion detection and prevention programs run out of the Department of Homeland Security (DHS) that seek to protect federal government networks; proposals for the government to play a similar protective role for private networks related to defense and other critical infrastructure; and legislative efforts that would promote sharing of cyber security data between the private sector and the government. The Einstein programs monitor government networks for cyber security. Einstein 1 and Einstein 2 are intrusion detection systems, which analyze network traffic traveling to and from participating government agencies. The programs screen for network traffic, which can include personally identifying information, but neither stops any traffic. Einstein 3 goes a step further; it is designed to prevent an intrusion by malicious code, rather than merely detect it. To do this, it delays the traffic headed for government computers temporarily for screening and then either lets it proceed or, if it has identified malicious code, quarantines that data. Einstein 3 screening takes place outside of federal networks, on the servers of Internet Service Providers (ISPs).

The privacy community, though wary of these programs, has generally accepted them for a variety of reasons. First, they relate only to traffic on government systems and do not involve monitoring of private sector networks. Second, DHS has been transparent about the programs and their proposed operation, releasing a series of detailed Privacy Impact Assessments that describe the programs. Also, the Justice Department's Office of Legal Counsel released its opinions explaining the legal basis for the programs. And, importantly, the government has taken privacy concerns into account in the development of these efforts and has minimized government collection and use of private data.

The privacy perspective is not incorporated effectively in the very early stages of developing technology, programs, or policy, when it could be the most helpful.

Another effort, this time to promote security in certain private sector networks, likewise has met with general approval by the privacy community. The effort known as the Defense Industrial Base (DIB) Pilot, began in 2011 as a trial program to assist companies that contract with the Defense Department in protecting their networks. The Department of Defense ran the program initially, but management has since been transferred to DHS. Early concepts for this program would have made the NSA responsible for identifying and preventing malicious intrusions on private networks. As the plan developed, however, it shifted away from government presence in the private systems and instead relied on the government providing threat information to the companies, who use it to defend their own systems. Any sharing of information from the private sector to the government is voluntary. The resulting program has been praised in the privacy commu-

nity as a way for the government to help private sector networks do a better job of protecting themselves, while avoiding the temptation to create a collection program.

Most controversial from a privacy perspective has been proposed cyber security legislation that would, in part, promote sharing of cyber security information between the private sector and the government. Significant efforts to pass such a bill in 2012 failed. A Senate cyber bill that the Administration actively supported and privacy advocates generally approved was voted down, largely for reasons unrelated to privacy. Most recently, on April 22, 2013, the House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA). The privacy community had strongly opposed an earlier version of this bill. Although the new version made a number of accommodations to privacy concerns, the privacy community still opposes it and the Obama administration has threatened a veto. In this version, the authors of the bill eliminated a significant role for the NSA in information sharing, which had been a major sticking point. But remaining concerns include that the legislation does not place adequate requirements on the private sector to strip out identifying information when possible, and that it lacks sufficient controls on subsequent use of private information that the government receives.

The government must do a better job of incorporating privacy into policy and technology development from the outset.

The Senate continues to work on cyber legislation, but prospects are dim for anything passing this year. The Snowden leaks surely have not helped. But the privacy community had already been an effective voice on cyber issues, so even without Snowden, legislation would not have made progress without addressing privacy concerns. Similarly, other cyber security initiatives, particularly those that contemplate a broader role for the NSA, will surely be put on hold—but they probably would not have moved under any circumstances.

MOVING FORWARD

The cyber security story is not an entirely happy one. Those who believe the government should be playing a more active role in protecting private sector networks, and in particular that the NSA—recognized as the government's expert on cyber matters—should not be sidelined, are deeply frustrated with the current situation. But there is some promise in the cyber security example: the Einstein and DIB programs demonstrate that the national security and privacy communities can sometimes communicate effectively. In the long run, though, real improvement requires a change in the approach of both groups.

First, the government simply must get better at being transparent about its use of data and the legal analysis that supports that use. This will not be easy. Rampant public skepticism notwithstanding, details of most intelligence programs are classified because to reveal them makes the programs less effective. The instinct of the intelligence community to protect details of these programs from disclosure is entirely rational. But in order to increase public trust, that instinct must be examined, second-guessed and tempered. The public will rarely be satisfied for long with general assurances that the government is protecting its privacy. This is particularly true when it comes to legal analysis. The criticism of "secret law" that followed Snowden's leak of an order from the FISC has been particularly damaging.

In addition, the government must do a better job of incorporating privacy into policy and technology development from the outset. President Obama has announced the creation of a position for a privacy and civil liberties officer at the NSA, which addresses this need. But the government also can do a better job of turning its immense creativity and technical expertise to the development of tools that address privacy concerns. For example, NSA Director General Keith Alexander recently expressed his openness to examining mechanisms that would allow the agency to analyze data without collecting it all in its own databases. Other avenues for innovation might be audit technology and anonymized analytics.

For its part, the privacy community must do a better job of adjusting to the explosion of data availability in our society. It is increasingly unrealistic to protect privacy primarily by prohibiting government collection of personal

data when that data is so widely available to the private sector and others. Although the government must temper its desire to collect everything into its own databases, it should not be expected to forgo the powerful national security resource that data collections represent. Although it challenges traditional notions of protecting privacy—which equate privacy with anonymity—the privacy community should focus more on imposing controls on how human beings in the government can access and use information that resides in databases and less on keeping data away from the government entirely. ■

ENDNOTES

[1] "House Narrowly Votes Down Move to Gut NSA Collection Program," nbcnews.com, July 24, 2013, http://nbcpolitics.nbcnews.com/_news/2013/07/24/19658896-house-narrowly-votes-down-move-to-gut-nsa-data-collection-program?lite.

[2] Letter to senators dated June 25, 2013. Available online at https://www.cdt.org/files/pdfs/Letter-Senate-Cybersecurity-Privacy.pdf.

[3] Greg Nojeim, "Cyber Security and Privacy: We're Watching," Center for Democracy and Technology (blog) June 25, 2013, https://www.cdt.org/blogs/greg-nojeim/2506cybersecurity-and-privacy-were-watching

[4] This term refers to groups for whom privacy is a key concern: privacy advocates, liberals, libertarians, and many in the technology community.

[5] The report of the "Church Committee" chronicles pervasive abuse over many decades of the privacy and liberties of U.S. citizens at the hands of the FBI, CIA, NSA, and the U.S military. See United States Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Intelligence Activities and the Rights of Americans, bk. 2 (Washington, DC: 1976) (final report, issued April 26, 1976).

[6] Department of Homeland Security, "Privacy Impact Assessment (PIA) 3-Year Review (Einstein)," June 28, 2013, http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-einstein-june2013-3-year-review.pdf ; Department of Homeland Security, "Privacy Impact Assessment (PIA) 3-Year Review (Einstein 2)," June 28, 2013, http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-einstein2-june2013-3-year-review.pdf.

[7] The Department of Homeland Security (DHS) began rolling out Einstein 3 in late July, 2013. See Amber Corrin, "DHS Rolls Out Einstein Intrusion Detection," FCW, July 26, 2013, http://fcw.com/articles/2013/07/26/einstein-rollout.aspx.

[8] Department of Homeland Security, "Privacy Impact Assessment for EINSTEIN 3," April 19, 2013, http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf.

[9] Department of Homeland Security, "Privacy Documents for the National Protection and Programs Directorate (NPPD)," n.d., http://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd.

[10] Department of Justice, Office of Legal Counsel, "Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch," January 9, 2009, http://www.justice.gov/olc/2009/e2-issues.pdf; Department of Justice, Office of Legal Counsel, "Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch,' August 14, 2009. http://www.justice.gov/olc/2009/legality-of-e2.pdf

[11] It has been renamed the Joint Cyber Security Services Pilot.

[12] See Patriots Debate: Contemporary Issues in National Security Law (American Bar Association, 2012), chapter 6, http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch6/ch6_ess2.html

[13] Cybersecurity Act of 2012, S. 3414, July 23, 2012, http://www.govtrack.us/congress/bills/112/s3414/text.

[14] Cyber Intelligence Sharing and Protection Act, H.R. 624, April 22, 2013, http://www.gpo.gov/fdsys/pkg/BILLS-113hr624rfs/pdf/BILLS-113hr624rfs.pdf.

[15] David Sanger, "NSA Leaks Make Plan for Cyberdefense Unlikely," New York Times, August 8, 2013, http://www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyberdefense-unlikely.html?_r=0.

[16] Siobhan Gorman, "Pressure Builds for Data-Sweep Alternative," Wall Street Journal, July 19, 2013, http://online.wsj.com/article/SB10001424127887324448104578615881436052760.html.

THE LAW ON KILLER ROBOTS

CHARLI CARPENTER

In April 2013 Christof Heyns, the UN Special Rapporteur on Extrajudicial Executions, presented a path-breaking report to the United Nations Human Rights Council calling for a moratorium on the development and deployment of fully autonomous weapons systems (AWS).[1] The report suggests that AWS might hasten the rush to war, undermining the legal regime enshrined in the UN Charter. It also raises concerns about whether such weapons could comply with humanitarian law, and questions whether their use would create an accountability gap in the laws of war.

The UN is not alone in calling for attention to the legal and ethical implications of outsourcing targeting decisions to machines. In 2009, concerned scientists formed the International Committee for Robot Arms Control. Three years later, in 2012, Human Rights Watch released a report on the perils of fully autonomous weapons.[2] And in April of this year, an NGO campaign to ban AWS kicked off on the steps of Parliament in London. The campaign is endorsed by Nobel Laureate and renowned anti-landmine campaigner Jody Williams and now includes a coalition of over 30 NGOs. But a counter-movement of defense experts, international law specialists and roboticists argue that the legal issues are far from clear-cut, and that autonomous weapons might even comply better with international law than human soldiers.

ASKING THE RIGHT QUESTIONS

These developments raise many interesting questions about the relationship between advances in weaponry and the international legal system. What does the law say about new weapons? On what basis might a category of weapons be banned pre-emptively? Would the outsourcing of autonomous weapons make it more or less likely that governments could comply with existing rules of humanitarian and human rights law?

The first two questions are easy. Governments are required under Article 36 of the first additional protocol to the Geneva Conventions to determine whether the employment of a new weapon would, "in some or all circumstances be prohibited by any rule of international law." The U.S. is not a signatory to this particular protocol, but complies as a matter of policy with Article 36. New weapons are to be evaluated according to whether they meet the requirements of international humanitarian law, in particular the distinction and proportionality principles.

The proportionality principle states that the means and methods of war are not unlimited—and that some weapons, despite their military utility, may be unlawful if the suffering they inflict is unnecessary to achieve military objectives or disproportionate to their military importance. Previous rules against expanding bullets, designed to exacerbate injury, and blinding lasers, designed to cause permanent loss of sight, were created using this rationale. Yet some argue that autonomous weapons could be militarily necessary, or at least advantageous, when dealing with future cyber-attacks, in a political environment where casualty aversion makes it difficult if not impossible to quickly deploy sufficient troops. And it is unclear whether an argument can be made that the suffering they might inflict would be any more disproportionate than manned weapons in those scenarios.

The distinction principle requires weapons-bearers to distinguish civilians from combatants and direct their operations only at the latter; weapons incapable of distinguishing in this way are considered unlawful. Significant debate exists among roboticists and legal experts over whether fully autonomous weapons could ever meet

***Charli Carpenter** is a human security analyst and Professor of International Affairs at University of Massachusetts-Amherst, where she teaches courses on the rules of war. She is the author of three books on the protection of civilians and blogs at Duck of Minerva.*

this criteria. Techno-optimists like roboticist Ronald Arkin argue an autonomous system might be a superior ethical governor in conflict zones. [3] But roboticist Noel Sharkey argues that artificial intelligence could never reasonably replace human judgment in contexts where discrimination is difficult.[4] Others, like US Naval War College Professor Michael Schmitt have argued that even if autonomous weapons could never reliably tell civilian from combatant they might still be used lawfully in areas where civilians are not present, such as the open sea or outer space.[5] Questions about whether such systems could be controlled once deployed also come into play in the distinction discussion. Different points in this debate are subject to disagreement about the likely capacity of future technology.

Significant debate exists among roboticists and legal experts over whether fully autonomous weapons could ever sufficiently distinguish between civilians and combatants.

In the absence of a crystal ball, the debate has begun to center around whether in situations of such uncertainty where there seems a significant, path-dependent risk of public harm, governments should be permitted to proceed unchecked in military research or slow down. The Heyns Report's call for a moratorium represents a call for a precautionary principle—that untrammeled development, transfer or use of these systems should be suspended until these ethical issues are resolved.

LEGALITY AND MORALITY

But citing a different legal precedent, some campaigners are going farther: calling for a complete ban, a "red line" moral principle that keeps targeting decisions in the hands of human beings. The Campaign to Stop Killer Robots is a coalition of human rights and disarmament NGOs arguing that more is at stake than humanitarian principles in choosing whether or not to arm robots. The emphasis here is less on the question of whether machines can ever behave in accordance with the law, but whether a moral principle is at stake in outsourcing lethal decisions to computers. This argument was made most forcefully in a November 2012 Human Rights Watch report entitled Losing Humanity. If the issue is indeed one of morality—and survey data strongly suggests that many people believe it is—then this would constitute grounds for rules against killer robots, since the laws of war emphasize that the "principles of humanity" can be a basis for rules when codified international law provides insufficient guidance.

That public opinion is relevant in such matters is outlined in the famous Marten's Clause, inserted into the Hague Conventions as sort of a back-up plan for situations not foreseen by the drafters. It reads: "Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience."

By this logic, it is not simply a question of delaying these developments until suitable codes of conduct can be created. It is a question of making a collective choice to keep warfare in the hands of human beings with human moral judgment. And in invoking the language of "humanity" NGOs are also connecting this discussion to wider bodies of law beyond those typically used to regulate war. War law applies only to armed conflicts and only under very specific conditions, regulating behavior between very specific groups of people: foreign soldiers and foreign civilians. But human rights law regulates not armed conflict but rather how governments treat their own citizens.

Some have argued that international law should recognize a "human right not to be killed by a machine." When asked to explain their opposition to autonomous weapons, numerous survey respondents in the U.S. invoked fears not of battlefield conditions gone awry but of domestic government tyranny aided by autonomous robotic police, executioners, or national guardsmen. It is telling that the first UN report on this subject came

not from a humanitarian law body like the Office for the Coordination of Humanitarian Affairs but rather a body tasked with enforcing human rights law.

When asked to explain their opposition to autonomous weapons, numerous survey respondents in the U.S. invoked fears not of battlefield conditions gone awry but of domestic government tyranny aided by autonomous robotic police, executioners, or national guardsmen.

FUTURE UNCERTAIN

Because there is no precedent for such a debate—earlier pre-emptive bans dealt with weapons clearly shown to violate the proportionality principle—it is difficult to know how it will shake out. One thing is for certain, however; autonomous weapons are not "inevitable," as some claim. The global community has often banned weapons and other technologies based on moral concerns. Blinding lasers, expanding bullets, chemical weapons, and cluster munitions are all now prohibited by treaty law, and ethical debates in areas like human cloning demonstrate that just because humans can do something doesn't mean they will. ■

ENDNOTES

[1] Christof Heyns, "Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions," United Nations Human Rights Council, April 9, 2013.
[2] Losing Humanity: The Case Against Killer Robots (New York: Human Rights Watch, 2012).
[3] Ronald Arkin, "The Case for Ethical Autonomy in Unmanned Systems," Journal of Military Ethics 9, iss. 4, 2010, 332-341.
[4] Noel Sharkey, "Saying No To Lethal Autonomous Targeting," Journal of Military Ethics 9, iss. 4, 2010, 369-383.
[5] Michael Schmitt, "Autonomous Weapons Systems and International Humanitarian Law," Harvard National Security Law Journal, 2013, http://harvardnsj.org/wp-content/uploads/2013/02/Schmitt-Autonomous-Weapon-Systems-and-IHL-Final.pdf.

ADAPTING AMERICAN SPACE SECURITY STRATEGY

JEFF KUETER

Over the decades since Sputnik catalyzed space as an arena for international security competition, there has been much continuity to U.S. space security policy. Historian Cargill Hall summarized the core principles of U.S. space policy this way:

...for fifty years, between 1955 and 2005, a few basic principles have undergirded U.S. space policy, principles enumerated in presidential NSC [National Security Council] space directives from Eisenhower to Clinton. During this period they have remained remarkably consistent, with the United States pledged to freedom of space, that is, free access to and unimpeded passage through space for satellites of all nations and to the exploration and use of space for peaceful purposes for the benefit of all mankind. (The terms "peaceful purposes," then and today, embraced defense-support activities including intelligence.) Second, the U.S. rejected any claims of sovereignty over outer space or other celestial bodies; third, it pursued three interrelated government space programs, civil, military and intelligence; fourth, it recognized the space systems of all nations as national property with the right of passage through and operation in space without interference (purposeful interference with operational space systems was and remains viewed as an infringement on sovereign rights); and fifth, the U.S. reserved the right to conduct, if attacked, activities in outer space in support of self-defense.[1]

Hall's assessment was prepared before release of the last two national space policies and the associated space security strategies and related documents that elaborate on these principles and their interpretation. The policy of the George W. Bush administration was said to be aggressive and unilateralist, while the Obama administration's policy struck an inclusionary tone with its embrace of international consensus on norms and rules as a primary means for securing a stable space security environment. But these different approaches reflected an enduring reality. The struggle for U.S. policymakers remains to craft a policy architecture that reflects the realities of how the U.S. military is exploiting space to its advantage with technical, budgetary, and diplomatic priorities.

WHY MILITARY SPACE MATTERS

Space systems today help to meet five principal military missions: (1) environmental monitoring, (2) communications, (3) position, navigation, and timing; (4) integrated tactical warning and attack assessment; and (5) intelligence, surveillance, and reconnaissance. These missions are integral to a new American way of warfare. Uniquely, the U.S. military has successfully integrated space-provided information into and with its conventional warfighting capabilities. Space enables the warfighter to be more precise in the prosecution of attacks, reducing the probability of unintended damage while also reducing risks of casualties. But, along with these advantages are new risks and new threats to U.S. security.

Other external forces are combining to lead to a critical juncture for U.S. investments in national security space capabilities. The convergence of three forces is bringing these concerns into focus. First, the fundamental shift in U.S. defense and diplomatic strategy from the western to the eastern Eurasian landmass—the so-called "pivot" toward the Asia-Pacific, where a larger geographic expanse and a rapidly maturing space competitor (China) present new, unique challenges to the use of space. Second, a large number of the national security space

Jeff Kueter *is President of the George C. Marshall Institute. He works with scientists to help improve the understanding and awareness of complex scientific topics to the public, the media, and policy makers. Mr. Kueter has served as Research Director at the National Coalition for Advanced Manufacturing (NACFAM) and at Washington Nichibei Consultants.*

capabilities upon which the United States and its allies critically rely are now legacy systems in need of upgrades and replacement. Third, severe fiscal pressures on Department of Defense and intelligence community budgets limit opportunities for new investment and support for new technologies.

The struggle for U.S. policymakers remains to craft a policy architecture that reflects the realities of how the U.S. military is exploiting space to its advantage with technical, budgetary, and diplomatic priorities.

As the strategic context shifts, the military's dependence on space systems becomes ever more acute. Since the 1990s, military use of space has grown exponentially, but new strategic demands, bolstered by the accumulating demands of technology, require new focus on space.

This growth in demand and axiomatically increased dependence will intensify as defense budget cuts compel forces stripped of manpower and capabilities to leverage space systems as an ever greater force multiplier. Designing a strategy to protect, preserve, and utilize America's advantages in space must recognize and accommodate these larger forces while also appreciating those factors unique to operating in outer space.

MYRIAD CHALLENGES

Protecting space assets presents complicated challenges. Foremost among the questions to be considered is what should be protected along with the related concern of protected from what threat(s)? No conflict will be decided in space. Space is important for what it enables, but conflicts are resolved on the ground. Consequently, the impact of any attack on, destruction of, or denial or degradation of service from a space asset is significant only to the extent that terrestrial warfighting capabilities are adversely impacted. For any given scenario, judgments about the impact of degraded access to space assets or their outright destruction on the mission needs of the joint fight are required. This requires in-depth knowledge both of the operations of the satellites, downlinks, data analysis and dispersion, but also how that information is used by troops in the field, their commanders, and others. A robust space security strategy would support a comprehensive assessment of the integrated impact of space-enabled information.

Armed forces fight the way they train. A fear arising from the U.S. military's dependence on space-enabled information is that in a time of crisis the denial or degradation of space will yield large effects. Space security strategies must recognize these dependencies and ensure that U.S. forces train to develop and employ work-arounds for space systems that are degraded or denied to them.

To some extent, these efforts are underway today. But the alternatives to space systems, such as high-altitude surveillance from drones or terrestrial/cable IT networks, are expensive, sometimes slower, and less responsive than comparable space assets. Additionally, sometimes the alternatives are themselves dependent on space systems. In the case of drones, if they are used as replacements for targeting purposes, their use of communications satellites to transmit data could also prove problematic in certain space warfare scenarios. Whether a given alternative is a viable replacement to a comparable space system, then, turns on how successfully it can be integrated and used in a timely manner. More work is needed to fully understand the alternatives to space systems, their limitations and their utilities.

Space systems face physical and electronic threats. Satellites can be destroyed damaged by objects running into them whereby the kinetic energy created by the collision destroys both objects. China's anti-satellite (ASAT) tests over recent years are a recent example of this approach. Objects exploded in the vicinity of a satellite can create damaging debris fields. The Soviet Union had developed a co-orbital high-energy fragmentation ASAT. Electronic threats, such as jamming or "spoofing" information transmissions or blinding the satellite, offer more accessible means to challenge U.S. use of space. Electronic approaches rarely inflict physical harm to the satellite and are more transitory in their effects. They also are more difficult to attribute. Consequently, they are an attractive alternative for many nations concerned about the

U.S. or other nation's military use of space.

Protecting space assets from physical attacks presents complicated problems. For example, to safeguard an individual satellite from a kinetic attack from a Chinese-like ASAT, which is a warhead launched from the ground designed to intercept a satellite at a specific point in space, one could move the satellite by changing its orbit or altering its speed. Either would likely result in a missed interception, since the interceptor likely lacks the sensory awareness to close in on the satellite once it has moved, or would run out of fuel before it could do so. But moving a satellite also has consequences. Satellites have limited fuel supplies themselves and moving them in response to threats shortens their operational lives. Further, altering orbits may also impact the satellite's ability to perform its mission. In the case of a surveillance satellite, movement from one place changes what it sees on the ground. A robust missile defense capable of global coverage offers additional protection from a ground-launched ASAT.

Space security strategies must ensure that U.S. forces train to develop and employ work-arounds for space systems that are degraded or denied to them.

More worrisome for space protection are the problems presented by a revived Soviet-style, clandestinely-placed, co-orbital or proximity ASAT whose presence would not be known until it is used. Aside from steps to harden or otherwise improve on-orbit survivability, little could be done to protect a satellite. Improved awareness of the space environment is the best approach to defend against this prospective threat, and with it comes the added benefit of improved protection from space debris or accidental collisions. Prioritizing the deployment of additional on-orbit sensors to aid in-space observations of critical assets ought to be a priority of a U.S. space security strategy.

Defending U.S. satellites from jamming or other electronic threats is similar to physical protection approaches. The most direct protection uses electronic means to defeat or evade the jamming, which are run from ground stations. An enemy cannot jam a satellite that it cannot locate. Moving satellites that come under electronic assault offers immediate defense. As the U.S. develops new generations of satellites, it can introduce new designs and use materials that make them difficult to find—just as it has done with airplanes, ships, and submarines. Understanding how prospective adversaries undertake space surveillance would directly contribute to those efforts and would be a priority for U.S. security.

Finally, surveillance and situational awareness forms a critical backbone of U.S. security in space. Knowing where objects are while keeping its systems hidden provides major advantages to the U.S., particularly while satellites remain highly vulnerable assets. But that strategic imperative conflicts with other stated goals for space. Commercial entities have an interest in knowing where other objects are to avoid collisions with satellites or other debris, for example.

CHARTING A DIFFERENT PATH

In order "to foster global spaceflight safety and help prevent mishaps, misperceptions, and mistrust," the U.S. National Security Space Strategy advocates sharing situational awareness information with others.[2] The International Code of Conduct also makes shared situational awareness of space objects an obligation of those who agree to the Code.[3] Whether unilaterally as a consequence of policy, in response to commercial pressures, or as a result of diplomatic commitments, the U.S. risks directly or indirectly sacrificing a most significant means of defense in space as more accurate "maps" of satellite locations become widely available.

The Obama administration has pledged U.S. support for the Code of Conduct and the underlying rules of the road and norms of responsible behavior that it believes will provide the basis for a more stable space security environment. Such a move jeopardizes rather than strengthens U.S. interests in space as it requires the U.S. to agree to a general framework before the detailed obligations are understood. Put simply, there are other, more transparent means to achieve the desired end. U.S. strategy should reject the Code and other arms control approaches.

Most satellites are largely indefensible and the means to replace them are problematic. Satellites take considerable time to manufacture, launching them takes time and careful planning, and both are extraordinarily expensive. In addition to aforementioned hiding and moving approaches, space security planners are evaluating new architectures for future constellations of satellites that offer redundant capabilities by employing more, smaller, and hopefully cheaper individual assets. By dis-

More work is needed to fully understand the alternatives to space systems, their limitations and their utilities.

aggregating the missions formerly met by a single, larger satellite onto many platforms, the attacker is also forced to launch ever larger efforts to degrade U.S. capabilities, supporters claim. While future security strategies must carefully examine the benefits of smaller satellites and distributed constellations so too should the costs of this approach be weighed in the balance.

Finally, active defense of critical assets warrant additional consideration in U.S. space security planning. Active defense, through the use of nano satellites to perform counter-kinetic kill operations, present significant technical challenges and today are quite costly. As the security environment evolves and technology matures, the situation may change. A comprehensive space security strategy would include an active and robust active defense effort to ensure the U.S. remains at the leading edge of those developments.

The security challenges faced by the U.S. in space will only deepen in complexity and sophistication in the years to come. No international agreement or treaty will solve the puzzle of managing security competition in this new arena. America's long-term interests in space are best preserved through concentrated capabilities, resilient systems, and vigilant defense.■

ENDNOTES

[1] Richard H. Buenneke, Richard DalBello, R. Cargill Hall, and Roger D. Launius, "National Space Policy: Does it matter?" May 2006:8, http://www.marshall.org/pdf/materials/439.pdf

[2] U.S. Department of Defense, "Fact Sheet: Space Situational Awareness (SSA)," 2011, http://www.defense.gov/home/features/2011/0111_nsss/docs/SSA%20Fact%20Sheet%20FINAL.pdf.

[3] Secretary of State Hillary Clinton, "Press Statement: International Code of Conduct for Outer Space Activities," January 17, 2012, http://www.state.gov/secretary/rm/2012/01/180969.htm.

GLOBAL MARITIME CHOKEPOINTS: DYNAMICS AND THREATS

JEFF M. SMITH AND JARED SWANSON

No spotlight on the global commons would be complete without a review of a key potential flashpoint: global maritime trade chokepoints. Although such bottlenecks abound in international waters today, four in particular stand out because of their geostrategic importance and their central role in the world economy.

Chokepoint	Annual Petroleum Traffic	Width (narrowest point)	Sovereignty (in nearby waters)	Alternatives
Straight of Hormuz	17 million barrels per day (mbpd)	21 miles	Oman, Iran, UAE	Iraqi, Saudi, UAE pipelines (1 to 4 mbpd capacity)
Straight of Malacca	15 mbpd	1.5 miles	Malaysia, Indonesia, Singapore	Sunda and Lombok Straits in Indonesia
Bab el Mandeb Strait	3.4 mbpd	18 miles	Yemen, Djibouti, Eritrea	Suez Canal, Cape of Good Hope
Suez Canal	3 mbpd (4.5 with SUMED pipeline)	1,000 feet	Egypt	SUMED pipeline, Cape of Good Hope

STRAIT OF MALACCA

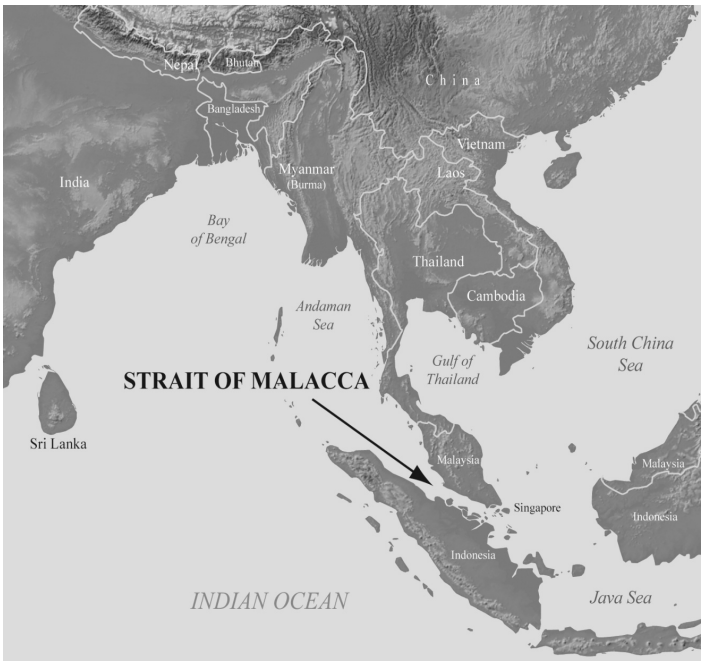
The Strait of Malacca remains the shortest navigable route for commercial traffic connecting the Indian and Pacific Oceans. A quarter of all oil carried by sea passes through the Strait: roughly 15 million barrels per day. In total, fifty thousand ships and 40% of world trade transit the Strait annually.

The Strait of Malacca is 550 miles long, but only 1.7 miles wide at its narrowest point (at the Phillips Channel), and dotted with thousands of small islets. At 25 meters deep, the Strait cannot service the largest crude carriers, but Very Large Crude Carriers (VLCCs) and Ultra Large Crude Carriers (ULCCs) can take an alternative, albeit longer route through the Lombok Strait to the south and east—adding, on average, three days to a ship's journey.

Management of the Strait falls to the three littoral countries—Singapore, Malaysia, and Indonesia—which have been fiercely protective of their sovereignty in the waters of the Strait and have implemented an elaborate set of cooperative mechanism and confidence-building measures to manage security in the Strait.

The highest-profile threat to shipping through the Malacca Strait in recent years stems from piracy. Piracy in the Strait peaked in the mid-2000s, when it accounted for nearly half of all pirate attacks worldwide. Indonesia is regularly identified as the most pirate-affected country in the world: out of 325 reported pirate attacks in 2004, 93 were in Indonesian waters[1]. However, a series of cooperative security initiatives implemented by the littoral states with help from Thailand, India and others have caused a sharp decrease in piracy attacks since 2005. These initiatives include the Malacca Strait Sea Patrols, Eyes in the Sky, the Intelligence Exchange Group, the Tripartite Technical Experts Group, and the Asia Maritime Security Initiative. By 2011, as a result of these measures, the Strait had reached a "close-to-zero incident level."[2]

Jeff M. Smith *is the Director of South Asia Programs and Kraemer Strategy Fellow at the American Foreign Policy Council.* ***Jared Swanson*** *is a Research Associate at the Council.*



STRAIT OF HORMUZ

Arguably the most important energy chokepoint in the world, the majority of oil exports originating in the Persian Gulf pass through the Strait of Hormuz on their way to the Arabian Sea and beyond. This encompasses, on average, 17 million barrels of oil per day (including 20% of oil traded worldwide, 35% of all seaborne oil that is traded, and 10% of oil consumed by the U.S.).

The Strait is only 21 miles wide at its narrowest point, though it is deep enough to accommodate the largest crude carriers in the world. The 12-mile territorial seas of Iran and Oman overlap at the narrowest points of the Strait, but both shipping channels lay to the south in Oman's territorial waters, where the waters are deepest.[3] Eastbound traffic out of the Persian Gulf to the Indian Ocean traverses a two-mile-wide shipping lane just north of two small Omani islands, known as Great and Little Quoin, while a lane farther north handles westbound shipping into the Persian Gulf.

Though there is no precedent for a complete closure of the Strait of Hormuz, Iran has repeatedly threatened to do so in response to sanctions or to threatening military action by the United States[4]. The Islamic Republic, moreover, has significant capacity to do so. As the New York Times notes, "for two decades Iran has been investing in the weaponry of 'asymmetric warfare' – mines, fleets of heavily armed speed boats and anti-ship cruise missiles hidden along Iran's 1,000 miles of Persian Gulf coastline."[5] The country also employs midget submarines and is believed to have as many as 5,000 mines.[6]

Estimates regarding the length of time Iran could enforce a closure of the Strait range from a few days to a few months. But, as Joint Chiefs Chairman General Martin Dempsey notes, "the simple answer is, yes, they can block [the Strait of Hormuz]." However, Dempsey also notes that America has "invested in the capabilities to ensure that if [Iran blocks the Strait of Hormuz], we [the U.S.] can defeat that."[7]

The consensus among naval analysts is that "while Iran's naval forces could inflict damage [on the U.S.], they would ultimately be destroyed" in the event of a maritime confrontation. Moreover, Iran is as economically dependent on the Strait as any country—perhaps even more so. It has no substantive alternative means to export its crude oil (which makes up 76% of Iran's export earnings and 62% of government revenues[8]), and relies heavily on the Strait to import refined oil products.[9] It also would have to conduct its anti-access operations in Omani territorial waters. Therefore, experts have assessed that Tehran is unlikely to close or impede traffic through the Strait except as an act of extreme desperation.[10]

SUEZ CANAL

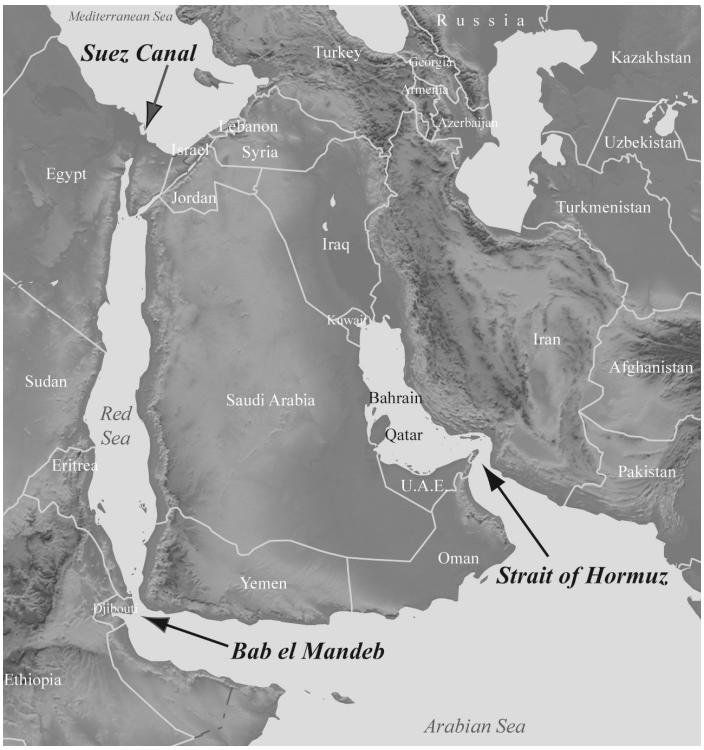
Connecting the Mediterranean to the Red Sea and Indian Ocean, the 100-mile long Suez Canal facilitates the passage of three million barrels of oil per day and eight percent of total global maritime trade. In total, 35,000 ships pass through the Canal each year, though only 10% are petroleum tankers. The Canal is only 1,000 feet wide at several points, and thus only able to accommodate one lane of traffic for many stretches.[11] The Canal is not deep enough to handle VLCCs and ULCCs, but a Suez-Mediterranean Pipeline (SUMED) bypassing the Canal can carry an additional 1.5 million barrels of oil per day. VLCCs will unload a portion of their oil into the SUMED pipeline to reduce weight, transit the canal, and

retake its crude at the other end of their pipeline.

The greatest risk for closure of the Canal comes from Egypt. As its sole owner and manager, Cairo is capable of closing off the Canal to traffic, and did so during the 1956-57 Suez Crisis. It accomplished this by sinking all 40 ships transiting the Canal at the time. Egypt again closed the Canal between 1967 and 1975 due to its two conflicts with Israel (the 1967 Six Day War and the Yom Kippur War in 1973)[12]. During the conflict in 1967, Egyptian forces also blockaded the Bab al Mandeb Strait to prevent supplies from reaching Israel.[13]

Egypt could use the Suez as leverage in any future inter-state conflict, including with Israel.

Hypothetically, Egypt could use the Suez as leverage in any future inter-state conflict, including with Israel. However, Cairo has enormous financial incentives to keep the Canal open, including annual government revenues of around $5 billion from taxes, tolls and surcharges.



Terrorism poses another, and potentially greater, threat to traffic through the Suez Canal. The Canal sits at the Western end of the Sinai Peninsula, a desolate, desert region of Egypt populated by Bedouins where state capacity is minimal. The traditionally lawless area has grown even more unstable since the 2011 revolution that overthrew longtime autocrat Hosni Mubarak in Cairo. In the more than two-and-a-half years since, violence and hostage-taking has spiked, with over 100 killed in the first eight months of 2013. Though it has not yet affected traffic in the Suez Canal in any major way, the possibility for disruption exists. For example, on August 31, 2013, a Chinese-owned container ship came under fire as it transited the Canal. Three suspects affiliated to a militant group in the Sinai Peninsula were arrested in connection with the incident.[14]

BAB EL MANDEB STRAIT

The "Gate of Tears" is the second chokepoint for ships passing to or from the Arabian Sea via the Suez Canal. Some 3.5 million barrels of oil per day pass through Bab al Mandeb, which connects the Red Sea to the Gulf of Aden. The Bab el Mandeb Strait is 18 miles across and hosts two navigational lanes divided by Yemen's Perim Island. The eastbound lane is two miles wide and 30 meters deep; the western route is 16 miles wide and 310 meters deep.

Piracy remains a concern to shipping through the Bab al Mandeb Strait due to its proximity to the Horn of Africa, which saw a considerable spike in pirate attacks in the mid-2000s following the Somali civil war. However, pirates have not been particularly active within the Strait itself, preferring to target ships in the open sea after they have cleared the passageway. In general, oil tankers tend to be too tall, and travel at speeds much too fast, to be subject to pirate attack.

Perhaps a greater concern stems from instability or state-failure in Yemen, where violent militant and separatist groups already operate in large ungoverned spaces. Al-Qaeda in the Arabian Peninsula, for example, enjoys a heavy presence in Yemen, where the group is headquartered. The perennially-troubled country was further destabilized in 2011 and 2012 when longtime

president Ali Abdullah Saleh was ousted, and long-term prospects for Yemen remain grim. Energy experts predict Yemen's oil supplies, which account for around 70% of government revenues, are likely to be exhausted within a decade.[15] Should the country descend further into chaos, the possibility for disruptions of trade flows through Bab el Mandeb cannot be ignored.

Nearly half of all oil consumed globally passes through one of the four chokepoints mentioned.

FUTURE DANGERS

As this review demonstrates, the healthy maintenance of world trade is dependent on a handful of strategically-vital naval chokepoints. Nearly half of all oil consumed globally passes through one of the four chokepoints mentioned above, creating powerful incentives for states to collaborate to ensure the security and vitality of these Sea Lines of Communication. This collaboration has proven particularly effectively in countering threats from non-state actors like pirates, most notably in the Strait of Malacca and off the Horn of Africa.

As a result, the greatest threats to these chokepoints in the start of the 21st Century stem from state actors themselves. Iran and Egypt both have the demonstrated capability to close the Suez Canal and Strait of Hormuz, respectively, though both have compelling financial incentives not to do so. The greatest threat to the Bab el Mandeb remains state failure in Yemen, while the Strait of Malacca is comparatively secure, given its joint management by the three littoral powers and the elaborate collaborative mechanisms currently in place. ■

ENDNOTES

[1] Benjamin J. Sovacool, *The Routledge Handbook of Energy Security* (London, England: Routledge, 2011).

[2] "Drastic Drop in Piracy in Malacca Straits," MaritimeSecurity.Asia. April 21, 2011, http://maritimesecurity.asia/free-2/piracy-2/drastic-drop-in-piracy-in-malacca-straits/.

[3] "Is the Strait of Hormuz Governed by Treaty or by Customary International Law?" The View from LL2, January 7, 2012, http://viewfromll2.com/2012/01/07/is-the-strait-of-hormuz-governed-by-treaty-or-by-customary-international-law/.

[4] Giacomo Luciani, "Restrictions of Passage, Accidents and Oil Transportation Norms Impact on Supply Security," Centre for European Policy Studies CEPS Working Document no. 354, June 2011, http://www.ceps.eu/book/restrictions-passage-accidents-and-oil-transportation-norms-impact-supply-security.

[5] Elizabeth Bumiller et al. "U.S. Sends Top Iranian Leader a Warning on Strait Threat," New York Times, January 12, 2012, http://www.nytimes.com/2012/01/13/world/middleeast/us-warns-top-iran-leader-not-to-shut-strait-of-hormuz.html?pagewanted=all&_r=0.

Tony Capaccio, "Keeping Strait Open to Get Tougher as Iran Expands Force" Businessweek, January 19, 2012, http://www.businessweek.com/news/2012-01-19/keeping-strait-open-to-get-tougher-as-iran-expands-forces.html#p1.

[7] Remarks of Gen. Martin Dempsey, Face the Nation, CBS, January 8, 2012, http://www.cbsnews.com/8301-3460_162-57354647/face-the-nation-transcript-january-8-2012/.

[8] Kenneth Katzman et al. "Iran's Threat to the Strait of Hormuz," Congressional Research Service, January 23, 2012, http://www.fas.org/sgp/crs/mideast/R42335.pdf.

[9] Luciani, "Restrictions of Passage, Accidents and Oil Transportation Norms Impact on Supply Security."

[10] See, for example, Daniel Lee, "Iran's Naval Ambitions," American Foreign Policy Council Iran Strategy Brief no. 7, September 2013, http://www.afpc.org/files/getContentPostAttachment/222.

[11] "A Deep Look At Oil Tankers And The Suez Canal In The Wake Of The Egyptian Crisis." Business Insider, February 7, 2011, http://www.businessinsider.com/a-deep-look-at-oil-tankers-and-the-suez-canal-in-the-wake-of-the-egyptian-crisis-2011-2.

[12] Luciani, "Restrictions of Passage, Accidents and Oil Transportation Norms Impact on Supply Security."

[13] David Cutler, "Factbox - Some facts on the Bab al-Mandab shipping lane," Reuters, June 4, 2011, http://uk.reuters.com/article/2011/06/04/uk-yemen-shipping-bab-al-mandab-idUKTRE75241G20110604.

[14] Jonathan Saul, "Shippers brace for more Suez turmoil after vessel attack," Reuters, September 2, 2013, http://www.reuters.com/article/2013/09/02/us-suez-shipping-risks-idUSBRE9810FA20130902.

[15] "United Nations Development Assistance Framework Republic of Yemen" United Nations Development Program. 2012-2015. January 2011. http://www.undp.org.ye/reports/Yemen%20-%20final%20signed%20UNDAF_January%202011.pdf.

THE FUTURE OF AMERICAN AIR POWER

MARK A. BUCKNAM

America's ability to dominate the airspace of its adversaries, and to use that airspace for military, counterterrorism, and intelligence-gathering purposes, is a cornerstone of U.S. national security. Cutting-edge fighter aircraft piloted by highly-trained American airmen have been the essential foundation upon which much of the modern-day U.S. security edifice has rested.

Yet America's repeated airpower successes in the decades since the Cold War ended have lulled some observers, including political decision-makers, into discounting the need to fund the continuous evolution of American fighter-aircraft capabilities. This is evidenced by the dramatically curtailed procurement of F-22 fighters and more recent challenges to the viability and affordability of the F-35. Notwithstanding criticisms that can be leveled against these pricey airpower platforms and expectations that they might soon be replaced by unmanned systems, U.S. security will continue to depend on maintaining its significant edge in high-tech fighters, the weapons they employ, and the well-trained airmen who operate them.

A WINNING TRACK RECORD

America's superior fighter aircraft technology, employed by highly-skilled airmen, has been essential to the success of U.S. military operations since the 1991 campaign against Iraqi military forces in Operation Desert Storm. As part of Desert Storm, 38 days of coalition air operations took control of the skies over Iraq, pummeled Iraqi military forces and leadership targets, and paved the way for a 100-hour air and ground operation that featured demoralized Iraqi soldiers surrendering to unmanned aerial vehicles. Modern American fighter aircraft, sometimes referred to as tactical aviation or TACAIR, flew over 75 percent of the missions employing ordinance in Desert Storm, and they executed nearly all of the missions employing precision-guided munitions (PGMs). The extremely low casualty rates among American fighters reflected tremendous advances in technology and extensive training built upon the lessons of the Vietnam War, and honed in years of preparation for conflict against the Soviet Union.

After Saddam Hussein's forces were ejected from Kuwait in 1991, American fighters spent more than a decade enforcing no-fly zones over portions of Iraq. From 1993 until 1995, U.S. tactical aviation enforced a no-fly zone over Bosnia. And in the summer of 1995, a 3-week NATO air campaign against the Bosnian Serb Army—called Operation Deliberate Force and conducted by a force overwhelmingly comprised of U.S. fighters—helped set the stage for the Dayton Peace Accords, ending Bosnia's bloody 3-year conflict. The near impunity with which high-tech American fighter forces operated over Iraq and Bosnia provided U.S., coalition, and NATO political leaders options to pursue political objectives at acceptable costs. Subsequently, in the spring of 1999, in Operation ALLIED FORCE, NATO airpower—with U.S. fighters executing the vast majority of missions—was an essential element in securing allied political objectives in Kosovo. The success of all three military campaigns—in Iraq, Bosnia, and Kosovo—hinged on the enormous advantages in survivability, precision, and raw numbers of sorties provided by American fighter forces.

Similarly, the more recent campaigns toppling the Taliban government in Afghanistan and Saddam Hussein's regime in Iraq owed their successes to U.S. fighter aircraft, their pilots, and weapon systems operators. Although bomber aircraft, gunships, attack helicopters, and other military platforms played vital roles at times, the vast majority of combat sorties were flown by American fighters and they delivered the overwhelming preponderance of precision munitions.

Mark A. Bucknam *is Chairman of the Department of Security Studies at the National War College in Washington DC. He retired from the U.S. Air Force as a colonel, after 30 years of service. A career fighter pilot, he also served in the Pentagon on the Air Staff, the Joint Staff, and in the Office of the Secretary of Defense, where was the Director for Campaign and Contingency Plans.*

While some senior U.S. military officials refer to the years since 9/11 as America's decade of war, American fighter pilots have deployed and operated through more than two decades of combat, starting with the first Gulf War and continuing to this day. There are two important reasons many observers overlook the first of those two decades: first, conventional U.S. ground forces were not involved in combat operations between DESERT STORM and IRAQI FREEDOM, and second, American combat airpower so dominated its adversaries that the risks associated with those air operations in the 1990s was judged to be low. Employing American airpower—primarily high-tech fighters—was politically expedient and nearly invisible to the public. The characteristics that make U.S. fighters so successful may now risk making America's airpower advantage a victim of its own success.

America's cutting-edge fighter technology has been, is, and will remain essential to success of major U.S. military operations.

A VICTIM OF ITS OWN SUCCESS?

In the hands of well-trained airmen, America's fourth-generation fighters—such as the F-15, F-16, and F/A-18—possess impressive capabilities and are highly survivable in combat. In addition to the excellent flying performance of these fighters, they are equipped with superior avionics, including radar, radar-warning equipment, sensors for locating and striking targets, and weapons control computers. Furthermore, these outstanding aerial platforms employ increasingly sophisticated weapons for air-to-air combat, suppression of enemy air defenses, and precision attack of ground targets day or night, in good or bad weather. Fighters are smaller and much more maneuverable than bombers and gunships, making them harder to detect and enhancing their survivability. They operate in larger numbers using tactics that can overwhelm or outsmart enemy defenses, and they can typically perform a variety of missions, thus giving military planners greater flexibility than do more specialized aircraft. And, in addition to protecting more vulnerable aircraft, modern high-tech fighters can usually defend themselves. In short, America's cutting-edge fighter technology has been, is, and will remain essential to success of major U.S. military operations.

Nevertheless, high-tech military hardware, particularly fighter aircraft, has long had its detractors. In the run-up to the first Gulf War, television networks and other media outlets found no shortage of doomsayers predicting rampant failure of modern weapon systems from the U.S. Army's M-1 Abrams tanks and AH-64 Apache attack helicopters, to the U.S. Air Force's F-15s and F-16s. Events proved those critics of high-tech weaponry wrong, yet some of the same critics have reemerged to drone once more against the unacceptable risks of depending on cutting-edge technology. To such critics, every setback or delay associated with pushing the boundaries of technology is seen as proof that systems are too complex to work or will prove too expensive.

Even before the 1991 Gulf War, the so-called Military Reform Movement offered in all seriousness the proposal of scrapping expensive high-tech fighters such as the F-15 for more numerous, low-tech aircraft such as the F-5 and even propeller planes reminiscent of the P-51s and P-47s of the Second World War. One shudders to think how such low-cost aircraft and their American pilots—assuming that in an all-volunteer force sufficient numbers of pilots could be found to operate such technologically inferior planes—would have fared against Saddam Hussein's forces in 1991, much less the more capable forces of the Warsaw Pact countries. To succeed in large-scale modern-day conflicts, or to be politically useful in more limited combat operations, U.S. fighter aircraft must possess capabilities and a degree of survivability that provides a very significant advantage over America's potential adversaries.

As today's budget cuts force the Department of Defense (DoD) to tighten its belt, TACAIR is likely to become a prime target. During the last Quadrennial Defense Review (QDR) in 2009 and 2010, sacrificing TACAIR was a bill-paying option of first-resort. Tactical aviation was seen as an area in which the United States possessed such superiority that it could afford to be cut without excessive risk to the nation. Notwithstanding the need

to make tough choices, during the QDR military force planners seemed to offer options for cutting fighters without regard to any limits to such cuts. Among the multitude of QDR studies, none examined the effects of such cuts on America's ability to execute its existing war plans or fulfill the needs of its global defense posture. As a consequence, the U.S. Air Force predictably found itself directed by DoD to cut fighter squadrons, then chastised at every turn when it did so. Air Force leaders were rebuked whenever the elimination of a particular squadron contradicted the force-posture aims of DoD policymakers, the force requirements of combatant commanders, or the imperatives of politicians whose Air National Guard forces were affected.

America's fighter overmatch could quickly erode. In late-February 2004, U.S. pilots flying the latest-model of the F-15C Eagle—America's premier air-to-air fighter at the time—were somewhat surprised and chagrined at the results of Cope India, a mock combat exercise against the Indian Air Force.

Undoubtedly, new studies are already underway for the 2014 QDR, and the design of those studies will impact decisions about how many and what type of fighters to buy. The most challenging high-intensity scenarios will feature potential adversaries with sophisticated anti-access/area-denial (A2/AD) capabilities. The value of fighter aircraft in such scenarios may be steeply discounted due to the limited range of fighters and the vulnerability of their bases. Of course, aerial refueling of distant land-based fighters and the basing of fighters on aircraft carriers would mitigate these limitations.

If these mitigating measures are deemed insufficient, suggesting the impossibility of operating effectively anywhere within hundreds of miles of an adversary's borders, then one should pause to consider exactly what political objectives one might hope to achieve and by what means. What is the point in having a scenario that admits no military solution as part of a defense review intended to reach decisions about force structure and strategy?

AN ERODING EDGE

But the truth is that America's fighter overmatch could quickly erode. In late-February 2004, U.S. pilots flying the latest-model of the F-15C Eagle—America's premier air-to-air fighter at the time—were somewhat surprised and chagrined at the results of Cope India, a mock combat exercise against the Indian Air Force. American pilots reported being impressed by the skills and tactics of the Indian pilots and more than a little concerned about what they observed from India's highly-capable Russian-made Su-30MK fighter aircraft. Of the 17 different types of fourth-generation fighters in the world, America fielded four. One of these, the F-14 Tomcat of Top Gun fame, is no longer in use. Reassuringly, the United States military still fields nearly 2,000 fourth-generation fighters and America leads the world in deploying fifth-generation fighters, with 186 F-22s in service today and hundreds of F-35 Joint Strike Fighter (JSF) aircraft scheduled to begin entering the inventory in the next few years. By comparison, Russia and China—with the 2nd and 3rd largest air forces, respectively—each field just over 500 fourth-generation fighters and have only recently begun testing prototypes of their fifth-generation fighters.

However, these figures are deceptive. America's fourth-generation fighters have been flown hard, are aging, and are in serious need of replacement. In 2009, the Obama administration, DoD, and the U.S. Senate acted in concert to halt production of the F-22 at 187 aircraft. This number is fewer than half of the 381 F-22s the U.S. Air Force deemed necessary in 2006, and well under one-third of the 650 aircraft the Air Force planned to buy around the time the Soviet Union collapsed in 1991.

The 2009 decision to curtail F-22 production was based largely on the expected capabilities and numbers of F-35 JSF aircraft that DOD planned to purchase; currently the Air Force is expected to receive 1,763 F-35s, with the Navy and Marine Corps getting 680. Prolonged delays in fielding the F-35 or significant cuts in their numbers could quickly erode America's impressive advantage in

fighters. Moreover, America's potential adversaries will likely shorten the U.S. lead in fighter technology given the rampant cyber-theft of American technology, including theft from U.S. defense contractors.

Fortunately for the United States, it also has a lead in well-trained airmen who can employ such technologically sophisticated aircraft.

THE HUMAN ELEMENT

America's fighter advantage depends as much on training and tactics as it does on technologically superior hardware. After the 1991 Gulf War, General Norman Schwarzkopf, the U.S. commander of all coalition forces, expressed his sense of the relative importance between training and technology in claiming that the superior training of American military forces was such that had the Iraqis and Americans exchanged equipment and fought the war, the American-led coalition would still have come out on top, and by a large margin.

Such superior training does not come easily. It takes two to three years to train a fighter pilot to the most basic level of combat readiness, with additional years needed to train a mission-ready wingman to be a flight lead, and then an instructor. Even an experienced community of fighter pilots can take many months to work out the best tactics for employing new capabilities, new weapons, or performing new missions in aircraft they are already skilled at employing. Reflecting on the implications of those last two sentences, one should readily see the flaws in thinking that the U.S. military could "skip a generation" of technology. Nor could the United States dramatically curtail the number of aircraft in the inventory with the hope of ramping up years later when a threat becomes imminent enough to spur action.

As American and British airmen learned at great cost in World War II, tactics and doctrine developed in the absence of robust training can turn out to be badly flawed. As a result, our airmen died in large numbers, even while flying some of the most technologically-advanced aircraft of their day. Ultimately, however, it was the Luftwaffe that demonstrated the steep cost of neglecting aircrew training; toward the end of the war, Germany possessed plenty of planes, including the first combat jet fighters, but nearly all of its experienced pilots were dead, and Germany had failed to train enough replacements. On D-Day, allied commanders were so confident they would control the skies over Normandy they ordered allied aircraft be marked with broad, highly-visible black and white stripes to avoid fratricide or friendly fire—they no longer worried about the Luftwaffe.

Those who think that drones, or unmanned combat aerial vehicles (UCAVs), will supplant America's fighter force in the next decade or so should think again. Unmanned aerial vehicles (UAVs) will certainly play an ever-increasing role in U.S. combat operations for many years to come. As they become more sophisticated, the types of missions they perform will continue to expand. The obvious advantages of UAVs—avoiding the loss of airmen and endurance—make them attractive to military planners and their political leaders alike. As the U.S. Navy conducts flight test operations with its stealthy X-47B UCAV, many observers will likely ponder, as The Economist editors did in 2011, whether the F-35 might be the last manned fighter. However, such unmanned aircraft are not cheap, and they still require human operators.

America's potential adversaries will likely shorten the U.S. lead in fighter technology given the rampant cyber-theft of American technology, including theft from U.S. defense contractors.

UCAVs will not supplant manned fighters until remotely-controlled vehicles can eclipse the skills demonstrated by on-scene humans in dealing with flight operations that are complex, dynamic, and inherently unpredictable. No analogy works perfectly, but consider the difficulty of designing and remotely operating a team of machines to play basketball against a skilled NBA team. Now, multiply that by ten such

games taking place simultaneously in close proximity to one another. An enormous difference exists between conducting a stealthy raid with a handful of UCAVs and engaging in aerial combat against a capable adversary.

The propensity to undervalue the sophisticated capabilities of human operators as compared to machines calls to mind an exchange that took place more than 30 years ago. In 1981, astronaut John Young, the captain of the first Space Shuttle mission, was challenged by a reporter to justify the need for manned space flight when computers were doing so much of the flying. Young responded with words to the following effect: where else are you going to get a 100-billion-bit computer that can reprogram itself in-flight and will work for forty-thousand dollars a year? Despite advances in computers, Young's message still rings true. No doubt technology will continue to advance in ways that make UAVs, including UCAVs, more competitive in performing missions that only people can perform well today, but in all likelihood the parents of the last American fighter pilot have yet to be born.

ENDURING LESSONS

In 1936, John Slessor—a veteran Royal Air Force (RAF) pilot of the First World War who rose to command the RAF after the Second World War—cautioned, "If there is one attitude more dangerous than to assume that a future war will be just like the last one, it is to imagine that it will be so utterly different that we can afford to ignore all the lessons of the last one." Given the vital role that America's fighter advantage has played in recent decades in underpinning the nation's security, it would be not only foolish but dangerous to surrender this edge.■

ENDNOTES

[1] Norman Schwarzkopf, Speech at the Miami Beach Convention Center, Miami Beach, Florida, January 22, 1992.

[2] "The Last Manned Fighter," The Economist, 14 July 2011, accessed at http://www.economist.com/node/18958487.

[3] Air Marshal, Sir John Slessor, Air Power and Armies (London: Oxford University Press, 1936), p. 62.

The views expressed in this article are those of the author and do not necessarily reflect the views of the U.S. Air Force, the National War College, or the Department of Defense.

Ilan Berman	Chief Editor
Rich Harrison	Managing Editor
Matthew Bodner, Harrison Menke, Alison Smith	Graphic Design and Layout

"Red World Map" cover art courtesy of Vector Templates

MANUSCRIPTS SHOULD BE SENT TO the attention of the Editor at 509 C Street, NE, Washington, DC 20002, or submitted via email to defensedossier@afpc.org. The Editors will consider all manuscripts received, but assume no responsibility regarding them and will return only materials accompanied by appropriate postage. Facsimile submissions will not be accepted.

EDITOR'S NOTE: The opinions expressed in the Defense Dossier (ISSN 2165-1841) are those of the author(s) alone and do not necessarily represent the opinions of the American Foreign Policy Council.

About the American Foreign Policy Council

For more than three decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

DEFENSE DOSSIER

American Foreign Policy Council
509 C Street, NE
Wahsington, D.C. 20002
www.afpc.org