2017 Award Winner
USAWC Student Awards Program

The Third Offset, Remotely Piloted Systems, and Moral Hazards

by

Mr. Mark Hamilton
Office of the Secretary of Defense

Under the Direction of:
Dr. C. Anthony Pfaff

United States Army War College
Class of 2017

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

The views expressed herein are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE	*Form Approved--OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 01-04-2017	**2. REPORT TYPE** STRATEGY RESEARCH PROJECT	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE The Third Offset, Remotely Piloted Systems, and Moral Hazards	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Mr. Mark Hamilton Office of the Secretary of Defense	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Dr. C. Anthony Pfaff	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution A: Approved for Public Release. Distribution is Unlimited. To the best of my knowledge this SRP accurately depicts USG and/or DoD policy & contains no classified information or aggregation of information that poses an operations security risk. **Author:** ☒ **PA:** ☒

13. SUPPLEMENTARY NOTES
Word Count: 5817

14. ABSTRACT

The Third Offset strategy is the Department of Defense's effort to develop future technical capabilities to ensure that it maintains its military advantage. However, it may engender two distinct, yet compounding, moral hazards. The first moral hazard considered originates from the Third Offset's technical focus. The Third Offset aims to reduce risks by increasing the effectiveness of weapons that remove the human warfighter from the battlefield. By distancing the human from conflict, this technology lowers not only the costs and risks associated with fighting, but the political "bar" to initiating hostilities as well. As a result, the U.S. government could inadvertently set conditions for an increase in international conflict. The second moral hazard results from the overt nature of the Third Offset's development. The unconcealed approach and design of the Third Offset raises the likelihood that American investments in defense modernization will inadvertently subsidize similar foreign efforts through espionage and foreign material exploitation of U.S. technological designs. These moral hazards, taken together could create a situation where U.S. defense efforts will inadvertently decrease global stability and national security.

15. SUBJECT TERMS
Drone, Ethics, Proliferation, Technology Loss

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU	29	**19b. TELEPHONE NUMBER** *(w/ area code)*

The Third Offset, Remotely Piloted Systems, and Moral Hazards

(5817 words)

Abstract

The Third Offset strategy is the Department of Defense's effort to develop future technical capabilities to ensure that it maintains its military advantage. However, it may engender two distinct, yet compounding, moral hazards. The first moral hazard considered originates from the Third Offset's technical focus. The Third Offset aims to reduce risks by increasing the effectiveness of weapons that remove the human warfighter from the battlefield. By distancing the human from conflict, this technology lowers not only the costs and risks associated with fighting, but the political "bar" to initiating hostilities as well. As a result, the U.S. government could inadvertently set conditions for an increase in international conflict. The second moral hazard results from the overt nature of the Third Offset's development. The unconcealed approach and design of the Third Offset raises the likelihood that American investments in defense modernization will inadvertently subsidize similar foreign efforts through espionage and foreign material exploitation of U.S. technological designs. These moral hazards, taken together could create a situation where U.S. defense efforts will inadvertently decrease global stability and national security.

The Third Offset, Remotely Piloted Systems, and Moral Hazards

The Third Offset strategy is the U.S. Department of Defense's (DoD's) effort to develop future technical capabilities to ensure that it maintains its military advantage. This strategy includes developing advanced remotely piloted systems (RPSs), autonomous systems, and artificial intelligence. Given that the Third Offset is a necessary endeavor, its technical focus and developmental approach may engender two distinct, yet compounding, moral hazards, which occur in situations where "greater risks are taken by individuals who are able to avoid shouldering the cost associated with these risks."[1]

The first moral hazard considered originates from the Third Offset's technical focus. The Third Offset aims to reduce risks by increasing the effectiveness of weapons that remove the human warfighter from the battlefield. By distancing the human from conflict, this technology lowers not only the costs and risks associated with fighting, but the political "bar" to initiating hostilities as well. As a result, the U.S. government could inadvertently set conditions for an increase in international conflict. Moreover, these offset technologies are derivatives from mature, commercial technologies and as such can be readily militarized and proliferated by other powers.

The second moral hazard results from the overt nature of the Third Offset's development. The unconcealed approach and design of the Third Offset, which distinguishes itself from previous offsets, raises the likelihood that American investments in defense modernization will inadvertently subsidize similar foreign efforts through espionage and foreign material exploitation of U.S. technological designs. These moral hazards, taken together could create a situation where U.S. defense efforts will inadvertently decrease global stability and national security.

Maintaining Overmatch Capabilities

After nearly two decades of the U.S.'s military engagements in the Middle East and Afghanistan, the world witnessed the awesome firepower, technology, techniques, and tactics that the U.S. can bring to the battlefield. Given the demonstrated abilities of the U.S. forces, near peer competitors such as the People's Republic of China and the Russian Federation modernized their military forces to achieve or exceed parity with the U.S. in key capabilities. As near peers modernized, the U.S. focused on operations and sustainment instead of maintaining its technological edge of major combat systems. Underscoring this point, on September 3, 2014 at the Reagan National Defense Forum, Secretary of Defense Chuck Hagel described the military's need to invest in a leap forward to the next set of technologies and processes to ensure the U.S. retains its competitive military advantage.[2] He described this technological edge as a way to offset the capabilities of near-peer competitors. This offset would avoid the costs of maintaining numerical parity of service members or weapons systems with a peer nation.

Seeking a historical context, Secretary Hagel labelled the U.S.'s planned employment of nuclear weaponry under President Eisenhower's "New Look Strategy" in the early 1950's, as the First Offset. The Second Offset was the development of stealth technology, precision guided munitions, and networked capabilities. As Secretary Hagel described it, the Third Offset will span the gamut of fields such as "robotics, autonomous operating guidance and control systems, visualization, biotechnology, miniaturization, advanced computing and big data, and additive manufacturing like 3D printing."[3] These offset technologies will enhance a broad range of future capabilities, to include RPSs, and further reduce operational risks.

RPSs – Air, Sea, and Land

The desire to reduce military operational risk by a RPS is not new. In 1849, the Austrian Army, under the command of Franz von Uchatius, used unmanned balloons with remotely activated bombs during the siege of Venice.[4] Since that time, the technology has significantly advanced. Today, service members located safely at locations such as Creech Air Force Base in Nevada, are piloting armed Reaper aircraft that are flying in Africa, Europe, and the Middle East.[5] While RPSs that operate in the air domain are in the public eye, there are also RPSs that operate in the maritime and land domains.

Since the 1970's, the U.S. Navy has been using unmanned systems for training and underwater mapping purposes.[6] In 2015, the Navy publicly announced its first operational use of an unmanned undersea vehicle (UUV), in which a submarine successfully launched and recovered.[7] The U.S. Army has also been investing in RPSs. Over the past decade, the Army invested in "more than 7,000 … items such as Talon IV, Packbot 510 FASTAC, SUGV 310 mini-EOD, Dragon Runner and First Look."[8] The majority of the Army's initial RPSs assisted with tasks such as explosive ordinance disposal and reconnaissance. However, the Army's designs and missions for RPS are evolving to include target acquisition with lethal and non-lethal effects.

Not surprisingly, this evolution of RPSs capabilities conforms to the DoD vision for unmanned systems. As found in the DoD Unmanned Systems Roadmap:

> The Department of Defense's vision for unmanned systems is the seamless integration of diverse unmanned capabilities that provide flexible options for Joint Warfighters while exploiting the inherent advantages of unmanned technologies, including persistence, size, speed, maneuverability, and reduced risk to human life. DOD envisions unmanned systems seamlessly operating with manned systems while

> gradually reducing the degree of human control and decision making required for the unmanned portion of the force structure.[9]

To get a sense of the financial costs associated with achieving that vision, DoD requested over $2.3 billion for the acquisition of the top three remotely piloted aircraft (RPA) in 2016. That request did not include funding for any of the other RPSs or for their associated research and development. This resource request provides insight into both the importance that DoD is placing on RPSs and the level of financial risks placed upon potentially fleeting technological superiority.

The Slippery Slope of RPSs

Regardless of the level of artificial intelligence or automation that unmanned platforms of the future may use, the physical distance between the service members and the area of conflict will increase. Given the reality of RPSs operating half a world away, it is not hard to imagine a future in which significant portions of the services' foreign combat missions are controlled by members that are safely protected in the homeland. Will this reduction in risk to service members' lives increase the U.S. penchants for using force? The Stimson Center, a nonpartisan policy research center that commissioned a task force to provide recommendations on the U.S.'s RPSs policy found that:

> The increasing use of lethal UAVs [unmanned aerial vehicles] may create a slippery slope leading to continual or wider wars. The seemingly low-risk and low-cost missions enabled by UAV technologies may encourage the United States to fly such missions more often, pursuing targets with UAVs that would be deemed not worth pursuing if manned aircraft or special operation forces had to be put at risk.[10]

A way to understand the possible increase in conflict enabled through RPSs is to examine historical examples and survey data that can provide insight into future RPS warfare.

In August 1998, there were two near simultaneous bombings of the U.S. embassies in Kenya and Tanzania in which intelligence quickly linked to Osama Bin Ladin.[11] President Clinton and his advisors wanted to retaliate against these bombings. Despite imperfect intelligence, two targets potentially linked to Bin Ladin quickly rose to the top of the list: a possible al-Qaeda camp in Afghanistan and a possible chemical weapon plant in Sudan.[12]

The President wanted to send a strong signal to Bin Ladin and retaliate with military force. However, there was hesitation by the senior military leadership to use ground forces.[13] This hesitation was largely due to the failed 1980 rescue attempt by the U.S. military elite unit Delta Force of U.S. hostages taken by Iran.[14] During the rescue attempt, multiple failures at a rally point 200 miles from Tehran led to the death of eight soldiers and caused senior leaders to abort the mission.[15] This failure may have influenced the exclusion of ground-based surgical strikes.[16] It may have also reinforced the desire to demonstrate action, yet limit operational risks, given the political ramifications that the U.S. hostage crisis had on President Carter's failed reelection bid.

A larger military force striking the two Bin Ladin linked targets would have compounded the operational risks. As then Secretary of Defense William Cohen told the [9/11] Commission, "the notion of putting military personnel on the ground without some reasonable certitude that Bin Ladin was in a particular location would have resulted in the mission's failure and the loss of life in a fruitless effort."[17] Committing aircraft to drop bombs would have required coordination with surrounding countries for both targets, complicating the operations and increasing risks to the pilots. However, the military now had Tomahawk Land Attack Missiles in its arsenal.

The use of Tomahawks allowed President Clinton to retaliate, without putting U.S. service members at risk. While not an RPS, these preprogrammed missiles can fly under radar systems, have a range of 700-900 nautical miles, and can deliver a 1000-pound bomb with an accuracy of 30 feet of a geographical target.[18] Less than two weeks after the embassy bombings, the U.S. launched 79 Tomahawks at sites in Sudan and Afghanistan.[19] This was not the first time that the U.S. had used Tomahawks to achieve a national security objective.

In June 1993, the U.S. struck the Iraqi Intelligence headquarters with 23 Tomahawks in retaliation for plotting to assassinate former President George H. W. Bush.[20] In both instances, the Tomahawks, given their accuracy and range, were the "safe" unmanned military options for the U.S. to achieve its objectives. Had unmanned military options not been available, it is doubtful that the President would have authorized the use of conventional forces in these incidences given the potential risks and the narrow scope of the objectives. This increased use of Tomahawks by the U.S. political and military leadership is an illustrative surrogate for the potential future growth of weaponized RPSs.

Since the U.S.'s first combat strike by an armed RPA in 2001, the use of armed RPAs has continued to rise.[21] As previously discussed, examining the DoD's Unmanned System Roadmap and budget reflect the importance of RPA in the military. While there is not a public database of all U.S. RPA strikes, on July 1, 2016 President Obama issued an executive order (EO) entitled *United States Policy on Pre- and Post-Strike Measures to Address Civilian Casualties in U.S. Operations Involving the Use of Force*. This EO requires the Director of National Intelligence (DNI) to report the "number of strikes undertaken by the U.S. Government against terrorist targets outside areas of active hostilities from January 1, 2016, through December 31, 2016" and to provide a yearly update thereafter.[22] In accordance with this EO, the DNI released a "Summary of U.S. Counterterrorism Strikes Outside Areas of Active Hostilities between January 20, 2009 and December 31, 2015." It listed 473 strikes, which resulted in an estimated 2372-2581 combatant deaths and 64-116 non-combatant deaths.[23] While these figures do not explicitly state that they were all RPA strikes, there is a high probability that the U.S. conducted them with RPA since they exclude strikes inside the controlled airspaces of Afghanistan, Iraq, and Syria. Consider that prior to the use of RPA, a nation would have to risk the consequences of sending its military personnel to a foreign country to conduct 473 operations and kill over 2,000 foreign combatants. U.S. political and military leadership clearly appreciate the reduction in operational risks that RPS capabilities provide.

Recent surveys of the U.S. civilian population also reflected this desire to reduce operational risks to service members. The U.S. Pew Research Center survey found that 58% of the U.S. public approved of the U.S. conducting RPA strikes in countries like Pakistan, Yemen, and Somalia.[24] The authors James Walsh and Marcus Sculzke surveyed over 3,000 participants to quantify the propensity to support the use of force when using a low risk platform such as a RPA.[25] One of their findings was that "participants were more likely to support wars that posed lower levels of risk to American soldiers."[26] Jacquelyn Schneider and Julia Macdonald surveyed 2,148 U.S. citizens and found when "given a scenario with a high risk to air crew, 58 percent chose unmanned aircraft, while only 23 percent chose unmanned aircraft in the scenario specifying low risk to air crew."[27] These findings confirm that "casualty aversion" influences "when and how wars are waged in democratic societies."[28]

The public support for RPA strikes makes them more politically viable option. When coupled with the DoD's Unmanned Systems Roadmap, the question of "how" the U.S. will wage war in the future is clearly going to include some form of RPSs. The previously mentioned examples of the Tomahawk strikes and the DNI's report of 473 strikes outside of areas of active hostilities illustrate the use of these types of weapons in areas that the U.S. decided not to risk conventional ground forces. The lower the risk, the more likely countries will engage in conflict through armed RPSs.

RPSs undoubtedly reduce the risk to the service members, and therefore lessen the potential for social outrage directed at elected leaders. There may actually be a political and perverse incentive for elected leaders to use RPSs beyond the human considerations. As RPSs are used more frequently and in riskier situations than conventional forces, their rearming requirements increase and are more likely to require repairs or to be replaced, thereby stimulating jobs.

Proliferation

As the U.S. continues to rely on armed RPSs, the international community has taken notice. The reduced risked to the operators, the relative low cost to obtain armed RPSs, and the minimal infrastructure to employ them regionally makes RPSs appealing military tools. The New America Foundation's International Security Program reported that the following countries and non-state actors have used armed RPA in combat: U.S., Israel, the United Kingdom, Pakistan, Iraq, Nigeria, Iran, Turkey, Hezbollah, Hamas, and the Islamic State of Iraq and Syria.[29] New America also reported that 86 countries have an RPA capability, 19 of which have armed RPA.[30] Worldwide sales of RPA have become a big business, with an estimated growth potential of over $11 billion in 2026 from $6 billion in 2016.[31] The countries profiting the most from RPA sales include the U.S., Israel, China, Iran, and Russia.[32] With this worldwide growth in mind, the U.S. Department of State (DoS) has started taking steps to address the proliferation of RPA.

In October 2016, the DoS issued a *Joint Declaration for the Export and Subsequent Use of Armed or Strike-Enabled Unmanned Aerial Vehicles (UAVs)* with 51 other countries.[33] This declaration states, “the international community must take appropriate transparency measures to ensure the responsible export and subsequent use of these [UAVs] systems.”[34] These measures should be taken by the international community because UAV strikes “could fuel conflict and instability.”[35] The declaration outlined five key principles, “none of which should be construed to undermine the legitimate interest of any State to indigenously produce, export, or acquire such systems for legitimate purposes.” What constitutes legitimate interests, purposes, or sales is not clearly defined except "[t]hat the export of armed or strike-enabled UAVs should be done consistent with the principles of existing multilateral export control and nonproliferation regimes.”[36] While this is not a legally binding document and does not restrict “legitimate” sales of RPA, it is interesting who did not sign the document. Out of those nations who have used armed RPA, Israel, Pakistan, Iran, and Turkey did not sign, nor did Russia and China as the other top RPA proliferators. Given their status as the leaders in RPA sales, China, Iran, and Russia may not have signed as purely an economic decision or out of concern for their ability to counterbalance U.S. hegemony by strengthening relations with other countries or non-state actors.[37] As with every competitive market, the products, such as RPA or any of the other RPSs, will continue to evolve. One way to acquire the evolving technology is to leverage the research and development costs borne by others. Given the public nature of the Third Offset, other countries may view the U.S. as a target of opportunity to obtain advanced technology with minimal investment.

Undermining the Third Offset by Losing the Technological Advantage

Unlike the first and second offsets, Secretary Hagel took a different approach and advocated for the Third Offset technological advances in a much more open manner. The U.S. government's work on the atomic bomb and stealth technology were highly classified programs. The secrecy involved with development of the atomic bomb was significant. A 1945 *Time Life* article estimated that over 100,000 people were involved with various aspects of the atomic bomb effort, but only a few dozen knew the full scope of the project.[38] While not as extensive as the atomic bomb effort, the U.S. took great care to protect the full capabilities of stealth technology associated with the F-117A stealth fighter. While the desire to develop low observable or stealth aircraft has been present since the 1900's, the full capabilities of the F-117A stealth fighter remained a well-guarded secret from development, to acknowledgement of its existence, and then to ten years later when it transitioned out of its secrecy envelope.[39] Openly soliciting and urging commercial entities to work on technologies that will be used to "offset" the capabilities of U.S. military competitors risks the very nature of the investment of the offset. The openness of the Third Offset could fuel the proliferation of advanced armed RPSs and provide pathways leading to intellectual property loss and corruption of the technology, putting the taxpayers' "investment" in DoD's modernization efforts at risks.

Intellectual Property Loss

As the U.S. government and private entities invest billions of dollars in the research and development of the technologies that will support the Third Offset, foreign nations will attempt to obtain those advances through less expensive means such as computer network attacks, corporate mergers, or reverse engineering. These methods of intellectual property (IP) loss are not exclusively focused on the companies associated with the Third Offset. However, the lack of secrecy associated with the Third Offset risks the very nature of the “offset” itself. This risk becomes self-evident when the “world’s largest source of IP theft” is the Peoples Republic of China. The IP Commission Report estimated that China is responsible for 50 – 80 percent of the worldwide IP thefts.[40] These IP thefts not only affect the U.S. economy at a rate of “hundreds of billions of dollars per year” but also its ability to maintain a competitive edge.[41] Computer network attacks on the defense contractors building a fifth-generation U.S. Air Force fighter is cautionary example of a military technology loss that could also happen to the Third Offset technology.

On March 23, 2016, a Chinese national pled guilty to conspiracy to hacking U.S. defense contractors’ system in order to steal sensitive data for the China. This conspiracy lasted from 2008 to 2014 and targeted information on the “C-17 strategic transport aircraft and certain fighter jets produced for the U.S. military.”[42] From the design and the technological leap forward, it is widely assumed that the China’s stealth fighter, J-20, is based upon the stolen technology. Stealing advanced technology is but one way to get it. Another way to obtain a technical edge without the research and development costs is through corporate mergers and acquisitions (M&A).

As of September 2016, China had surpassed the U.S. as the top acquirer of foreign companies.[43] China's desire to obtain the IP from these foreign acquisitions aids in achieving its "Made in China 2025" vision. China's vision focuses its efforts on 10 sectors as enumerated below:

> 1) New advanced information technology; 2) Automated machine tools & robotics; 3) Aerospace and aeronautical equipment; 4) Maritime equipment and high-tech shipping; 5) Modern rail transport equipment; 6) New-energy vehicles and equipment; 7) Power equipment; 8) Agricultural equipment; 9) New materials; and 10) Biopharma and advanced medical products.[44]

While China's shift in M&A from the resource sectors to the sectors listed above could be seen as a natural evolution of its economy, it is possible that the announcement of the Third Offset influenced their targeted sectors.[45] This might be perceived as China's whole of government effort to obtain both an economic and military edge as all ten sectors have military crossover applications.

A recent example of China's focus on a crossover company was its desire to obtain the German company AIXTRON. AIXTRON is a leader in producing advanced gallium nitride epiwafers, which are extremely useful in military applications due to their heat and radiation tolerance.[46] While the German government initially approved the sale, President Obama rejected the inclusion of AIXTRON's U.S. business based upon the recommendation of the Committee on Foreign Investment in the United States (CFIUS).[47] The President concluded that the role China's government played in financing the AIXTRON acquisition bid and AIXTRON's advanced technology posed too great a risk to national security.[48] Unlike many U.S. partner nations, the U.S. has a process to assess and deny M&A that pose a risk to national security.

CFIUS is a U.S. Department of Treasury led interagency committee that reviews and assesses foreign M&A that may negatively affect national security.[49] In CFIUS's most recent Annual Report to Congress, it received 347 notices (or requests for review) from 2012 – 2014, and identified that China accounted for the largest share of those notices.[50] With CFIUS's deep insights into foreign acquisition of U.S. companies, it comes as no surprise that their report provided this response regarding a coordinated strategy to acquire critical technology companies as described below:

> Based on its assessment of transactions identified by the CFIUS for the purposes of this report, the U.S. Intelligence Community believes there may be an effort among foreign governments or companies to acquire U.S. companies involved in research, development, or production of critical technologies for which the United States is a leading producer.[51]

The overt nature of the Third Offset strategy and its focus on technologic advancements may provide foreign countries logical targets of interest for possible M&As.

Sales or transfers of military technology to other counties also increase the risk of technological loss. Despite formal agreements that restrict further resale or access to these technologies by third countries, U.S. has identified partner nations as sources of technology proliferation. This type of loss was never so apparent than when in 1993, the former Director of Central Intelligence James Woolsey testified to the U.S. Senate that Israel had provided China advanced weapons for years and that Israel was the prime source of China's cutting-edge technology.[52] The Science Applications International Corporation and the Defense Threat Reduction Agency's Advanced Systems and Concepts Office assessed that "[a]mong the advanced weapons and technological assistance Israel is believed to have provided to China are laser-guided armor-piercing warheads, surface-to-air missiles, electronic fire-control systems, night-vision equipment, communications systems, and anti-tank missiles." [53] Several of the advanced systems that Israel transferred to China either were copies of U.S. weapons or based upon U.S. technologies.[54] Due in part to these technology transfers and the technological assistance that Israel had planned to provide China, the U.S. temporarily halted Israeli participation in the U.S. fifth generation strike fighter, the F-35.[55] Even with trusted partners, it is impossible to ensure the non-proliferation of shared technology.

The final way to lose a technological edge is to lose physical control of the technology. When countries obtain access to foreign technology such as advanced weapons, platforms, or devices, they normally study them in order to replicate or defeat them. How intrusive or potentially destructive that examination will be is dependent upon the relationship between those two countries and the duration of access. When studying advanced foreign technology, something as unobtrusive as obtaining exact measurements of equipment can provide insight into its function or capability, while a more intrusive examination may provide enough details to allow a country to reverse engineer the technology. While maintaining physical control is an issue with any advanced military technology, RPSs are unique. By their very design, they function at some distance from their operator. Additionally, the military will use RPSs more frequently and outside of traditional combat areas due to their lower operational risks. These unique factors make RPSs more vulnerable for physical loss and possible exploitation by foreign countries than manned military platforms.

China is one country that is exceptionally adapt at capitalizing on exploitation opportunities. Some have suggested that China's YU-7 light anti-submarine torpedo was based upon their serendipitous acquisition of a U.S. Mark 46 torpedo, China's J-15 shipborne fighter was based upon a version of the Russian SU-33 fighter, and China's

HQ-7 air defense missile was based upon France's Crotale missile system.[56] Over the past seventeen years, there have been three very public examples of the U.S. losing physical control of technologically advanced hardware to its adversaries.

On April 1, 2001, a U.S. EP-3 maritime reconnaissance and signals intelligence turboprop aircraft and the People's Liberation Army Navy (PLAN) F-8II jet fighter collided in international airspace.[57] The PLAN jet was lost at sea, and the pilot of the U.S. EP-3 had to make an emergency landing in Chinese territory on Hainan Island. China released the EP-3 crew eleven days later after tense negotiations, but delayed the return of the plane despite the fact that it was repairable and able to be flown off the island.[58]

In a press release following the return of the EP-3 crew, Secretary of Defense Donald Rumsfeld stated that they were not able to complete the "destruction of the classified material and systems."[59] On June 11, 2001, China agreed to allow the U.S. technicians to disassemble the plane and fly it out in a cargo plane.[60] This allowed China the time to examine the sensitive signals intelligence collection system contained within the EP-3. A Congressional Research Service (CRS) report indicated that the EP-3 had undergone a "recent major upgrade known as the Sensor System Improvement," and that China "may have removed some electronic surveillance equipment."[61] China's lengthy period in which they retained the damaged EP-3 and their harassment of a manned military aircraft operating in international airspace highlights China's disregard of international norms.

China once again disregarded international norms when they illegally seized a UUV on December 15, 2016. United States Naval Ship (USNS) Bowditch, an oceanographic survey vessel, was recovering two UUVs in the international waters of the South China Sea. As it was in the process of recovering the first UUV, a Chinese naval vessel deployed a small boat and seized the UUV.[62] The Chinese did this despite the fact that they were in visual range of the Bowditch, and could clearly observe that the Bowditch was in the process of recovering the UUVs. The international community speculated that China's actions could have been in reaction to then President Elect Donald Trump's conversation with Taiwan's president, and Trump's comment that he "wouldn't feel bound by a one-China policy."[63] Given the public announcement of the Third Offset and its focus on autonomous systems, China may have wanted to assess the UUV's technology and the potential data that it gathered.

The most troubling aspect of the Chinese removing the UUV from international water was the relative impunity in which they did it. The U.S.'s reaction was to issue a formal diplomatic note demanding the return of the UUV. While China returned the UUV five days later, it set a precedent for future armed RPS transiting the global commons. As the U.S. improves its RPSs technology, it will have to develop measures to ensure that the resources invested in the research and development of these advanced RPSs are not lost by another nation just plucking the RPSs out of the water.

The need for developing countermeasures to prevent technology loss was no more evident than in December 2011, when a U.S. RQ-170 stealth reconnaissance RPA crashed in Iran.[64] The RQ-170 is one of the U.S.'s premier reconnaissance RPA. Its advanced technology - from its design and special coatings to the advanced internal sensors - was far beyond Iranian technology. Official U.S. sources stated that it crashed landed due to an internal malfunction, though the Iranians claimed that they were able to bring the RQ-170 down by hacking into its communication and its guidance systems.[65] What made this situation particularly troublesome was that the Iranians found the RQ-170 intact. This gave the Iranians access to the data, the exquisite technology, and the potential for reversing engineering the RQ-170.

Concerns of the loss of technology were proven valid when in February 2013, the Iranian government published footage recovered from RQ-170. They demonstrated their ability to access the stored memory of the RQ-170 by showing "footage recorded by the drone's underbelly camera: the area surrounding Kandahar airfield (KAF) during landing; a small building (possibly being surveilled); a C-130 cargo plane, and at least one Reaper drone among shelters at KAF."[66] In May 2014, the Iranian government released pictures of a stealth RPA that they claimed they built by reverse engineering the captured RQ-170.[67] Less than two years after publicizing the Iranian copy of their stealth RPA, they released a video that showed a modified stealth RPA which was armed with four precision-guided bombs.[68] This example clearly demonstrates the concerns associated with losing physical control of advanced RPS technologies in the hands of another nation. Because of the loss of the RQ-170, Iran was able to shorten their RPA design timelines and build an armed stealth RPA on the research and development costs borne by the U.S. taxpayers.

Corruption of the Technology

If a country has detailed knowledge of a system such as a RPA, then it may be possible to insert counterfeit material into the supply chain in order to disrupt that RPA. The current path of the Third Offset as an open partnership with industry, coupled with the long development timelines, allows for strategic positioning by a foreign nation to influence the supply chain of the offset technologies. Security of the supply chain is vital for the economy of the U.S. as a whole, and it is critical for the U.S. military. Looking at the current state of counterfeit material in the DoD supply chain provides a good exemplar of this possibility. In 2016, the U.S. Government Accountability Office issued a report to Congress that stated:

> the existence of counterfeit parts in the DOD supply chain can, for example, delay missions, affect the integrity of systems, and ultimately endanger the lives of service members. Almost anything is at risk of being counterfeited, including microelectronics used in fighter jets and missile guidance systems, fasteners used in aircraft, and materials used in engine mounts.[69]

Counterfeit material is a problem throughout all of DoD. A 2012 report from the Senate Armed Serves Committee investigation identified “approximately 1,800 cases of suspect counterfeit electronic parts. The total number of individual suspect parts involved in those cases exceeded one million.”[70] While costs and profits drive the use of counterfeit material, it is not much of a stretch to consider the possibility of a country inserting material into the supply chain with the intention to cause a weapon like RPS to malfunction at a critical point.

Another concern is the possibility of inserting malicious code into the technology. Today’s modern weapons systems are laden with electronics that depend on lines of code. The more complex the equipment and interoperable it is, the more lines of code that it has. For example, “[t]here are nine million lines of code in the F-35 joint strike fighter jet, plus 15 million lines in support systems, according to Richard Stiennon, chief research analyst at IT-Harvest.”[71] It is easy to anticipate that as RPSs become more autonomous, the amount of code necessary to make them function will skyrocket. Without the proper safeguards in place, the opportunity will exist to modify or insert malicious code that could turn a RPS against its users.

Recommendations

The rationale for the DoD Unmanned Systems Roadmap and the technologies associated with the Third Offset is to reduce risks to U.S. forces by developing and enhancing armed RPSs that operated effectively in the air, sea, and land domains. However, this path is not without its own risks to larger national security concerns: increased international conflict, proliferation of armed RPSs, and international efforts to purloin the Third Offset technologies. The U.S. can take steps now that will help mitigate these risks, which include reassessing the long-term impact of using armed RPSs outside of combat zones, strengthening international agreements on the use and proliferation of armed RPSs, and enhancing the protection of the U.S.'s Third Offset investments.

The U.S. should factor in the long-term consequences of RPSs use along with risk assessment of the immediate operation. RPSs use outside of areas in which conventional military forces are operating are redefining international norms and lowering the bar for missile strikes. The lower threshold for strikes is not in the U.S.'s long-term interest as the U.S. may not be as effective in defending itself against future armed RPSs.

As the U.S. reexamines its own use of armed RPSs, it should work towards a formal international agreement on the legal use of all armed RPSs and their sales. The continued migration of this technology into the hands of terrorist is alarming. The *Joint Declaration for the Export and Subsequent Use of Armed or Strike-Enabled Unmanned Aerial Vehicles (UAVs)* acknowledges this problem of proliferation and is a step in the right direction.

Finally, in order to retain the advanced capabilities associated with the Third Offset, the U.S. should increase the physical and cyber security of critical technologies and systems during their development, production, and employment. Recent history has highlighted the fleeting nature and vulnerabilities associated with advanced military technologies. The U.S. cannot afford to have its technological edge undermined.

Conclusion

The Third Offset strategy is critical for the US to reestablish military overmatch with near peer competitors. Armed RPSs will be a significant component in this overmatch. Like guns, bombers, and destroyers, RPSs are very effective at their root objective as they allow the attacker to project force from a safe distance. It can also be argued that RPSs have a secondary benefit. Citing the DNI's report as evidence, supporters can claim that RPSs lower the risks of non-combatant deaths.[72] RPSs enable the operators to make more informed choices of when to strike due to their long loiter times and surveillance capabilities as compared to manned systems.

However, the moral hazards remain. The horrors of war are largely borne by the enemy on the ground, as well as any noncombatants in the vicinity, not the service members operating remotely from a base far away. Advances in RPSs, both in types and in capabilities, will continue to lower the risks associated with mounting an offence. Therefore, they will allow the use of force more frequently. As advanced RPSs are used more frequently, it increases the risk of losing that technological edge and increases the potential for proliferation. If the U.S. fails to consider the long-term consequences of using armed RPSs or fails to protect the technology as recommended above, it will find itself continuing to face these moral hazards and risks the very purpose of the Third Offset strategy.

Endnotes

[1] John Kaag and Sarah Kreps, "The Moral Hazard of Drones," *The New York Times Online*, July 22, 2012, https://opinionator.blogs.nytimes.com/2012/07/22/the-moral-hazard-of-drones/?_r=0 (accessed March 25, 2017).

[2] Charles Hagel, "Reagan National Defense Forum Keynote," public speech, Ronald Reagan Presidential Library, Simi Valley, CA, November 15, 2014, http://www.defense.gov/News/Speeches/Speech-View/Article/606635 (accessed September 15, 2016).

[3] Robert O. Work, "The Third U.S. Offset Strategy and its Implications for Partners and Allies," public speech, Willard Hotel, Washington, DC, January 28, 2015, http://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies (accessed September 18, 2016).

[4] Russell Naughton, "Hargrave - Remote Piloted Aerial Vehicles: An Anthology," http://www.ctie.monash.edu/hargrave/rpav_home.html#Beginnings (accessed September 18, 2016).

[5] Brian Everstine, "Inside the Air Force's Drone Operations," *Air Force Times*, June 22, 2015, https://www.airforcetimes.com/articles/inside-the-air-forces-drone-operations (accessed January 7, 2016).

[6] Michael Melia, "Submarine Launches Undersea Drone in a 1st for Navy," *The Navy Times Online*, July 20, 2015, http://www.militarytimes.com/story/military/tech/2015/07/20/submarine-launches-undersea-drone-in-a-1st-for-navy/30442323/ (accessed January 7, 2016).

[7] Ibid.

[8] David Vergun, "More Ground Robots to Serve alongside Soldiers Soon," *The Army Times Online*, April 8, 2015, https://www.army.mil/article/146061/More_ground_robots_to_serve_alongside_Soldiers_soon (accessed January 8, 2017).

[9] James A. Winnefeld, Jr., and Frank Kendall, "Unmanned Systems Integrated Roadmap FY 2011-2036 (Washington, DC: U.S. Department of Defense), http://www.acq.osd.mil/sts/docs/Unmanned%20Systems%20Integrated%20Roadmap%20FY2011-2036.pdf (accessed September 16, 2016).

[10] John Abizaid and Rosa Brooks, *Recommendations and Report of the Task Force on US Drone Policy*, 2nd ed. (Washington, DC: STIMSON, April 2015), 11, http://www.stimson.org/sites/default/files/file-attachments/recommendations_and_report_of_the_task_force_on_us_drone_policy_second_edition.pdf (accessed January 4, 2015).

[11] Michael Barletta, "Chemical Weapons in the Sudan: Allegations and Evidence," *The Nonproliferation Review Online* 6, no. 1 (Fall 1998): 116, http://www.nonproliferation.org/wp-content/uploads/npr/barlet61.pdf (accessed January 9, 2017).

[12] Ibid.

[13] Thomas H. Kean and Lee Hamilton, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004), 136, http://govinfo.library.unt.edu/911/report/911Report.pdf (accessed on March 3, 2017).

[14] Ibid., 96.

[15] Ibid.

[16] Ibid.

[17] Ibid., 136.

[18] U.S. Navy, "Tomahawk Cruise Missile," http://www.navy.mil/navydata/fact_display.asp?cid=2200&tid=1300&ct=2 (accessed January 10, 2017): Tony DiGiulian, "United States of America, Tomahawk BGM-109 Cruise Missile," *NAVWEPS Online*, http://www.navweaps.com/Weapons/WMUS_Tomahawk.php (January 10, 2017).

[19] Tom Vandern Brook, "Cruise Missiles are Accurate but are they Effective?" *USA Today Online,* August 28, 2013, http://www.usatoday.com/story/nation/2013/08/28/syria-cruise-missiles-chemical-weapons-bashar-assad/2720959/ (accessed January 10, 2017).

[20] Ibid.

[21] Chris Woods, "The Story of America's First Drone Strike," *The Atlantic*, May 30, 2015, http://www.theatlantic.com/international/archive/2015/05/america-first-drone-strike-afghanistan/394463/ (accessed January 10, 2017).

[22] Barack Obama, *Executive Order -- United States Policy on Pre- and Post-Strike Measures to Address Civilian Casualties in U.S. Operations Involving the Use of Force* (Washington, DC: The White House, July 1, 2016), Sec. 3.

[23] James R. Clapper, *Summary of Information Regarding U.S. Counterterrorism Strikes Outside Areas of Active Hostilities Online* (Washington, DC: Director of National Intelligence, July 1, 2016), 1, https://www.dni.gov/files/documents/Newsroom/Press%20Releases/DNI+Release+on+CT+Strikes+Outside+Areas+of+Active+Hostilities.PDF (accessed January 10, 2017).

[24] Pew Research Center, *Public Continues to Back U.S. Drone Attacks* (Washington, DC: Pew Research Center, May 28, 2015), 1, http://www.people-press.org/files/2015/05/5-28-15-Foreign-Policy-release.pdf (accessed March 5, 2017).

[25] James Igoe Walsh and Marcus Sculzke, *The Ethics of Drone Strikes: Does Reducing the Cost of Conflict Encourage War? (*Carlisle Barracks, PA: U.S. Army War College Press, September 2015), 2.

[26] Ibid., 3.

[27] Jacquelyn Schneider and Julia Macdonald, *U.S. Public Support for Drone Strikes*: *When do Americans Prefer Unmanned over Manned Platforms?* (Washington, DC: Center for a New American Security, September 20, 2016), 4, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-DronesandPublicSupport-Final2.pdf (accessed March 5, 2017).

[28] Walsh and Sculzke, *The Ethics of Drone Strikes,* vii.

[29] *New America's International Security Program, World of Drones Home Page,* http://securitydata.newamerica.net/world-drones.html (accessed March 1, 2017).

[30] Ibid.

[31] Katy Barnato, "'Growing Global Tension' to Drive Drone Sales, Seen Doubling by 2025: Research," *CNBC*, September 11, 2016, http://www.cnbc.com/2016/09/11/growing-global-tension-to-drive-drone-sales-seen-doubling-by-2025-research.html (accessed March 7, 2017).

[32] Robert Farley, "The Five Most Deadly Drone Powers in the World," *The National Interest*, February 16, 2015, http://nationalinterest.org/feature/the-five-most-deadly-drone-powers-the-world-12255?page=show (accessed March 5, 2017).

[33] The Joint Declaration signatories were Albania, Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Chile, Colombia, Czech Republic, Denmark, Estonia, Finland, Georgia, Germany, Greece, Hungary, Iraq, Ireland, Italy, Japan, Jordan, Kosovo, Latvia, Lithuania, Luxembourg, Malawi, Malta, Mexico, Montenegro, Netherlands, New Zealand, Nigeria, Norway, Paraguay, Philippines, Poland, Portugal, Republic of Korea, Romania, Serbia, Seychelles, Singapore, Slovakia, Slovenia, South Africa, Spain, Sri Lanka, Sweden, Ukraine, United Kingdom, U.S., and Uruguay. See U.S. Department of State, *Joint Declaration for the Export and Subsequent Use of Armed or Strike-Enabled Unmanned Aerial Vehicles (UAVs)* (Washington, DC: U.S. Department of State, October 28, 2016), https://2009-2017.state.gov/r/pa/prs/ps/2016/10/262811.htm (accessed March 7, 2017).

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Farley, "The Five Most Deadly."

[38] "Mystery Town Cradled Bomb: 75,000 in Oak Ridge, Tenn. Worked Hard and Wondered Long about Their Secret Job Online," *Life* 19, no. 8 (August 20, 1945): 108,111, https://books.google.com/books?id=hkgEAAAAMBAJ&lpg=PA25&pg=PA94#v=onepage&q&f=true (accessed January 10, 2017).

[39] Jim Cunningham, "Cracks in the Black Dike: Secrecy, the Media, and the F-117A," *The Airpower Journal*, Fall 1991, www.au.af.mil/au/afri/aspj/airchronicles/apj/apj91/fal91/cunn.htm (accessed January 5, 2017).

[40] Denis C. Blair and Jon M. Huntsman, *The IP Commission Report* (Washington, DC: The National Bureau of Asian Research, May 2013), 2-3,

http://www.ipcommission.org/report/ip_commission_report_052213.pdf (accessed January 16, 2017).

[41] Ibid., 2.

[42] "Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information," March 23, 2016, https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive (accessed January 16, 2017).

[43] Wade Shepard, "China Hits Record High M&A Investments in Western Firms," *Forbes*, September 10, 2016, http://www.forbes.com/sites/wadeshepard/2016/09/10/from-made-in-china-to-owned-by-china-chinese-enterprises-buying-up-western-companies-at-record-pace/#623a11b01387 (accessed January 16, 2017).

[44] Scott Kennedy, "Made in 2025," June 1, 2015, https://www.csis.org/analysis/made-china-2025 (accessed January 16, 2017).

[45] For information on "Made in China 2025", see *State Council of the People's Republic of China Special – Made in China 2025 Home Page*, http://english.gov.cn/2016special/madeinchina2025/ (accessed January 16, 2017): *China-Britain Business Council Made in China 2025 Home Page*, http://www.cbbc.org/mic2025/ (accessed January 16, 2017).

[46] Judy Lin, "Obama Blocks Grand Chip Investment Acquisition of Aixtron," *LEDinside*, December 7, 2016, http://www.ledinside.com/news/2016/12/obama_blocks_grand_chip_investment_acquisition_of_aixtron (accessed March 18, 2017); Paul Mozur, "Showdown Looms as U.S. Questions Chinese Deal for German Chip Designer," *New York Times Online*, November 19, 2016, https://www.nytimes.com/2016/11/20/business/dealbook/china-germany-aixtron-cfius.html?_r=0 (accessed March 18, 2017).

[47] "US Moves to Block Chinese Purchase of German Tech Firm Aixtron (Update) Online," *Phys.Org*, December 2, 2016, https://phys.org/news/2016-12-obama-blocks-takeover-germany-aixtron.html (accessed January 17, 2017).

[48] Ibid.

[49] The CFIUS interagency committee includes representatives from the Departments of Commerce, Defense, Energy, Homeland Security, Justice, State, the Intelligence Community (IC), and the Executive Office of the President.

[50] Committee on Foreign Investments in the United States, *Annual Report to Congress: Reporting Period: CY 2014* (Washington, DC: U.S. Department of the Treasury, February 2016), 3, 18.

[51] Ibid., 29.

[52] Dallas Boyd, Jeffrey G. Lewis, and Joshua H. Pollack, *Advanced Technology Acquisition Strategies of the People's Republic of China* (Ft. Belvoir, VA: Defense Threat Reduction Agency

Advanced Systems and Concepts Office and Science Applications International Corporation, September 2010), 27.

[53] Ibid.

[54] Ibid.

[55] Ibid., 28; *The Lockheed Martin F-35: Global Participation Home Page,* https://www.f35.com/global/participation/israel (accessed January 17, 2017).

[56] Boyd, Lewis, and Pollack, *Advanced Technology Acquisition*, 44, 45.

[57] Shirley A. Kan et al., *China-U.S. Aircraft Collision Incident of April 2001: Assessments and Policy Implications* (Washington, DC: U.S. Library of Congress, Congressional Research Service, October 10, 2001), 1.

[58] Ibid., 7.

[59] Ibid., 28.

[60] Ibid., 8.

[61] Ibid., 28.

[62] Missy Ryan and Dan Lamothe, "Pentagon: Chinese Naval Ship Seized an Unmanned U.S. Underwater Vehicle in South China Sea," *The Washington Post Online*, December 17, 2016, https://www.washingtonpost.com/news/checkpoint/wp/2016/12/16/defense-official-chinese-naval-ship-seized-an-unmanned-u-s-ocean-glider/?utm_term=.cefa406f33a9 (accessed January 19, 2017).

[63] Camila Domonoske, "China Seizes U.S. Underwater Drone from International Waters, Pentagon Says," *NPR*, December 16, 2016, http://www.npr.org/sections/thetwo-way/2016/12/16/505850933/china-seizes-unmanned-u-s-underwater-vehicle-in-international-waters (accessed January 17, 2017).

[64] Scott Shane and David E. Sanger, "Drone Crash in Iran Reveals Secret U.S. Surveillance Bid," *The New York Times Online*, December 7, 2011, http://www.nytimes.com/2011/12/08/world/middleeast/drone-crash-in-iran-reveals-secret-us-surveillance-bid.html (accessed January 17, 2017).

[65] Ibid.

[66] David Cenciotti, "IRAN RELEASES DECODED FOOTAGE FROM CAPTURED U.S (sic) STEALTHY RQ-170 DRONE," *The Aviationist*, blog entry posted February 6, 2013, https://theaviationist.com/2013/02/06/footage-sentinel/ (accessed January 21, 2017).

[67] David Cenciotti, "IRAN UNVEILS REVERSE-ENGINEERED VERSION OF CAPTURED U.S. RQ-170 STEALTH DRONE," *The Aviationist*, blog entry posted May 11, 2014, https://theaviationist.com/2014/05/11/iran-modified-version-rq-170/ (accessed January 21, 2017).

[68] David Cenciotti, "IRAN UNVEILS NEW UCAV MODELED ON CAPTURED U.S. RQ-170 STEALTH DRONE," *The Aviationist*, blog entry posted October 2, 2016, https://theaviationist.com/2016/10/02/iran-unveils-new-ucav-modeled-on-captured-u-s-rq-170-stealth-drone/ (accessed January 21, 2017).

[69] U.S. Government Accountability Office, *COUNTERFEIT PARTS - DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk* (Washington, DC: U.S. Government Accountability Office, February 2016), 1.

[70] U.S. Congress, Senate, Committee on Armed Services, *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain*, 112th Cong., 2nd sess., 2012, S. Rep 112-167, i-ii, http://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf (accessed January 21, 2017).

[71] Sean Lyngaas, "Untold Lines of Code Make Pentagon Weapons Vulnerable," *FCW*, June 3, 2015, https://fcw.com/articles/2015/06/03/pentagon-weapons-vulnerable.aspx (accessed June 28, 2017).

[72] Clapper, *Summary of Information*, 1.