NAVAL WAR COLLEGE

Newport, RI

The Targeting of U.S. Military Families by Foreign Governments

Word Count: 3396 words

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
14-05-2021	FINAL	N/A

4. TITLE AND SUBTITLE

The Targeting of U.S. Military Families by Foreign Governments

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Maj Frank Walker, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Writing & Teaching Excellence Center
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

A return to great power competition and the rise of destabilizing regimes in China and Russia brings competition for asymmetric military advantage and the blurring of traditional lines between criminal activity and legitimate military operations, in what is now understood as "*fifth generation* warfare." Foreign adversaries, unable to counter American military power directly, will seek alternate, indirect means to diminish U.S. power projection abroad. The increasing accessibility of military families, coupled with the relative ease of data collection and low-risk targeting opportunities, represents a new and extreme vulnerability. The Department of Defense must act quickly to provide legal, legislative, and cybersecurity protections to prevent coordinated attacks against military families.

15. SUBJECT TERMS (Key words)
Counterterrorism, China, Russia, Cyberwarfare, Force Protection, Operational Security, U.S. Military Families, fifth-generation warfare, asymmetric warfare.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	N/A	12	Director, Writing Center
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			19b. TELEPHONE NUMBER *(include area code)* 401-841-6499

Standard Form 298 (Rev. 8-98)

The United States has entered a period of renewed global competition with hostile near-peer rival nations. After nearly twenty years of unrivaled American military dominance following the fall of the Soviet Union and the end of the Cold War, both China and Russia have returned to the arena of great power competition to challenge the West diplomatically, economically, and in the cyber/information domains.[1] Even space is increasingly viewed as a potential battleground for anti-satellite warfare to deteriorate U.S. military technological advantages and deny access to regions of conflict.[2] There have not, however, been meaningful strides to challenge America's significant conventional military capability – at least not directly.

China and Russia are growing military powers, but pale in comparison to total U.S. military might.[3] Despite renewed Russian arms production and sales, Chinese naval shipbuilding programs, and the militarization of reefs in the South China Sea, the U.S. military stands generations ahead of the nearest-peer competitors in technology, training, doctrine, and integration.[4] So how will near-peer adversaries challenge the United States in the 21st century?

---

[1] The unclassified summary of the 2018 National Defense Strategy identifies "the *reemergence of long-term, strategic competition* by . . . revisionist powers and rogue regimes" such as China and Russia, and stresses the "decline in the long-standing rules-based international order" as the principal challenge to U.S. national security. (U.S. Secretary of Defense James Mattis, "Summary of the 2018 National Defense Strategy," *U.S. Department of Defense*, 2018.)

[2] Air Force Maj. Gen. DeAnna M. Burt, commander of the Combined Force Space Component Command at Spacecom, recently stated, "Spacecom's priorities are . . . keeping the space domain free and safe for all to transit and operate . . . [and] denying the enemy space-based capabilities, if necessary." (Vergun, David, "Spacecom Aims to Ensure Space Domain is Protected, General Says," *U.S. Department of Defense: DOD News,* May 2021, https://www.defense.gov/Explore/News/Article/Article/2593617/spacecom-aims-to-ensure-space-domain-is-protected-general-says/.)

[3] "The United States spends more on national defense than China, India, Russia, Saudi Arabia, France, Germany, United Kingdom, Japan, South Korea, and Brazil – combined." Further, the $732 billion dollar defense budget (2019) only "accounts for 15 percent of all federal spending" and "is currently below its historical average as a share of GDP." ("U.S. Defense Spending Compared to Other Countries," *Peter G. Peterson Foundation,* May 2020, https://www.pgpf.org/chart-archive/0053_defense-comparison.)

[4] The Brookings Institution assessed the U.S. military as being qualitatively ahead of China's, especially in areas of global power projection, "China does not seem to be in any huge hurry to build and flex its muscles. It is far away the world's #2 military power, but it only spends about one-third as much as the United States on its armed forces in absolute terms and only about one-half as much as a fraction of national economic output." (O'Hanlon, Michael E., "What the Pentagon's new report on China means for US strategy – including on Taiwan," *The Brookings Institution,* September 2020, https://www.brookings.edu/blog/order-from-chaos/2020/09/04/what-the-pentagons-new-report-on-china-means-for-u-s-strategy-including-on-taiwan/.)

Indirectly. With no potential to directly challenge U.S. conventional forces, hostile nations will increasingly seek innovative ways to neutralize American power projection by alternate, indirect means. Facing such a challenge, the U.S. military must begin an aggressive program of hardening the soft underbelly of support, sustainment, and readiness functions that allow expeditionary forces to project American military power abroad. Families represent one such gap, and perhaps no more sensitive "soft spot" exists in the hearts of America's warriors than the safety of their loved ones at home. U.S. servicemembers' families represent a critical vulnerability that hostile foreign governments and non-state actors could exploit to neutralize otherwise-protected, asymmetric U.S. military advantages. As such, in an age of indirect confrontation and with far fewer barriers to access and information, military families require better protection than ever before.

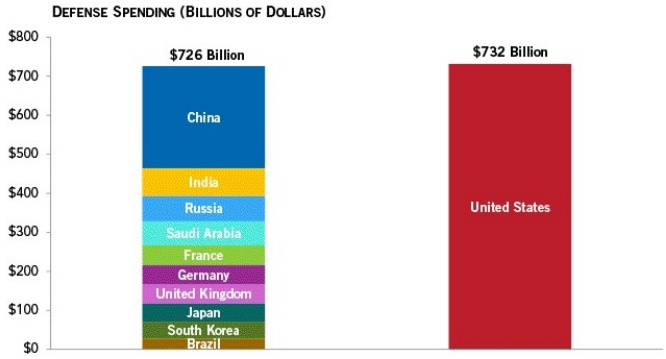

Figure 1 - The U.S. Military budget is larger than the next ten countries combined. (Source, Peter G. Peterson Foundation)

The Risk

The United States Government spends a considerable investment to maintain ready, responsive, expeditionary military forces around the world to respond to regional crises. Those forces cost time, manpower, training, and sustainment to guarantee U.S. power-projection across the globe. Moreover, the units closest to an emergent crisis are often several thousand miles away from significant U.S. and allied bases. As such, they represent the figurative "tip of the spear" for American intervention and cannot be easily supported, reinforced, or replaced in the time-competitive environment of early crisis-response. The Marine Air-Ground Task Force

(MAGTF) is one such organization. The typical MAGTF is the Marine Expeditionary Unit (MEU), with a Battalion Landing Team (BLT) as its primary ground combat element. The task force is spread across three U.S. Navy amphibious assault ships and prepared to conduct a range of military operations from humanitarian assistance to full-spectrum combat. Due to deployment and maintenance cycles, only two or three of these organizations are at sea at a time and strategically positioned across the world's oceans to provide maximum coverage for various potential emergencies. As a result, the risk of an indirect attack vector is that U.S. capabilities could be neutralized without being challenged militarily. Imagine the following scenario:

> *Under Presidential orders, the 11th MEU is directed to land the Battalion Landing Team, comprised of approximately 1,500 Marines and Sailors, in a growing crisis to prevent a neighboring regional power from seizing territory and locking the issue in a "frozen conflict." Suddenly, on the morning of the landings, Red Cross messages come flooding into the MEU command post afloat, alerting nearly a hundred servicemembers that their families have been killed or severely injured at their home station in Camp Pendleton, California, in what appears to have been a coordinated attack. With such heavy losses, including most of the Battalion's senior leaders, the 11th MEU is rendered combat ineffective. The next closest American forces will take more than a week to arrive.*

Framing the Problem

When conducting threat assessments, it is essential first to ask if the threat is reasonable. Is there any precedent for this type of attack? Allowing imaginations to run wild often results in costly and unnecessary security programs, but ignoring credible threats leads to catastrophic tragedies like the September 11th attacks or incidents of strategic surprise like Pearl Harbor. Like most matters of subjective judgment, threat assessments require a balance of credibility, cost, and risk.

Though the idea of foreign adversaries attacking military family members in the homeland is a difficult topic to discuss, the possibility deserves an honest assessment. Attacking families is nothing new in the long chronicles of warfare. For example, the Persians were on their way to attack Athenian families while the city's phalanxes were tied down at the Battle of Marathon in 490 BC. Nor is the idea new to use domestic sabotage to affect the withdrawal of troops from a combat theater, as when Imperial Japan funded domestic unrest in European-Russia to draw troops from Siberia during the Russo-Japanese War. The twentieth century is replete with further examples as nations shifted to total war and whole civilian populations became legitimate military targets. More recently, families were threatened and executed by insurgents in Iraq and Afghanistan to coerce tribal and government leaders.[5] [6] Russia targeted civilians in Chechnya, and the United Nations (UN) recently condemned Russia again for targeting civilians during its ongoing war in Ukraine.[7] [8] There is a clear historical precedent.

Figure 2 - Families and children are already on the front lines of Russia's war in Ukraine. (Source, Human Rights Centre ZMINA)

While this might seem a little far-fetched, nobody today questions the need to protect the President's and Vice President's, and other senior government leaders' families. However, this

[5] "Afghanistan: Targeted Killings of Civilians Escalate," *Human Rights Watch,* March 2021, https://www.hrw.org/news/2021/03/16/afghanistan-targeted-killings-civilians-escalate#.
[6] Roug, Louise, "Targeted Killings Surge in Baghdad," *Los Angeles Times,* May 2006, https://www.latimes.com/archives/la-xpm-2006-may-07-fg-civilians7-story.html
[7] Bouckaert, Peter, "War Crimes in Chechnya and the Response of the West: Testimony Before the Senate Committee on Foreign Relations," *Human Rights Watch,* February 2000, https://www.hrw.org/news/2000/02/29/war-crimes-chechnya-and-response-west.
[8] United Nations, "Pillay alarmed by killing of civilians in Ukraine," *United Nations Human Rights, Office of the High Commissioner,* August 2014, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14975.

practice only started after President McKinley's assassination in 1901. The threat is credible, and the cost sufficiently mitigates the risk. Heads of government remain high-value targets, but the shifting economics of indirect attacks make it increasingly likely that future adversaries may pursue this threat vector rather than attempt to confront U.S. military power directly.

In the past, human-intelligence (HUMINT) collection required to locate, track, and map transit routes, daily routines, and predictable points of vulnerability was expensive and time consuming. As such, it was a state-sponsored activity and only directed against national-level leaders. That began to change in the late twentieth century as the world became more accessible. For example, during the Arab-Israeli Six Day War, "Israeli intelligence had a clearer picture of the Egyptian order of battle and capabilities than did Egypt's own commanders." The head of Israeli military intelligence, Aharon Yariv, maintained, "'Know your enemy' was not . . . merely a figure of speech; it had to be taken literally. It was not enough to know Arab strategy on the grand scale; Yariv wanted to know everything about every Arab unit down to the menus served in the sergeants' mess." Due to the Israeli priority on preemptive strike against its Arab neighbors, Israeli intelligence services collected detailed information such as, "the whereabouts of every aircraft and name/information on the pilot; the name, background, status, and schedule of every base commander; reveille and morning schedules for the pilots and ground crews; [and] when senior air officials would be absent from their commands, and unable to direct operations."[9] This level of detailed information gave Israel a significant, asymmetric advantage during the 1967 conflict. It is easy to see how technological advances, the internet, and social media have made populations even more accessible in the intervening half-century.

[9] Elder, Gregory, "Intelligence in War: It Can Be Decisive," *U.S. Central Intelligence Agency, Studies in Intelligence, Vol 50, No 2,* 2006, https://apps.dtic.mil/sti/pdfs/ADA497904.pdf.

The means of collection are readily available. How would a potential adversary identify the units, specific personnel, key leaders, and locate their families? Much of this information is available online, through open-source collections. In the hypothetical scenario above, the units involved are easily identified by pre-deployment press releases, social media announcements to family members, and plenty of peer-to-peer social media interaction from the several hundreds to thousands of individual servicemembers preparing to deploy. Likewise, unit commanders, subordinate commanders, staff officers, and senior enlisted leaders are easily identified on the publicly accessible unit web pages. Many of those key leaders' professional biographies are also posted on unit web pages, with spouses and children identified by name.

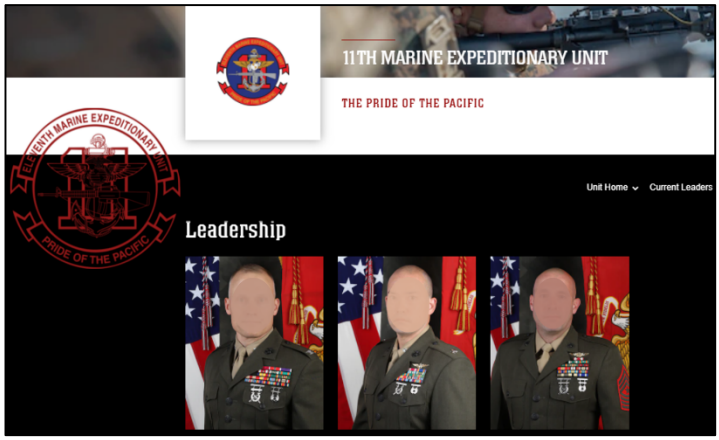

Figure 3 - Unit Leaders are easy to locate on publicly accessible unit websites and could be the first step in targeting vulnerable family members. (Source, 11th Marine Expeditionary Unit)

The ability to collect, locate, track, and attack low-level targets, like deployed servicemembers' families, already exists. Beyond the hypothetical scenario, a 2018 investigation by the New York Times found that commercially available smartphone application data could easily be correlated to identify an individual's device, despite being sold as anonymous user data. By focusing on the two most consistent locations, her home and place of work, the investigation was able to tie volumes of cell phone position data to an upper state New York schoolteacher, data that was collected and sold without her knowledge or consent. The data showed predictable tracks of her daily routine, the nights she made it to her Weight Watcher's meetings, nights she

skipped the gym, and even nights she stayed over at her ex-boyfriend's house.[10] Without greater regulatory protection for identifiable data, and with the ease of collection through open-source means, the entire networked population is easier to identify, locate, and track than ever before. Further, the specificity of commercially available user data simplifies the targeting process. What used to require extensive spy-networks to focus on limited, high-level targets can now be accomplished discreetly from a keyboard, without leaving the sanctuary of an adversary's national borders, and can be directed in a more general sense against larger groups of low-level American civilians to produce a disproportionate battlefield effect.

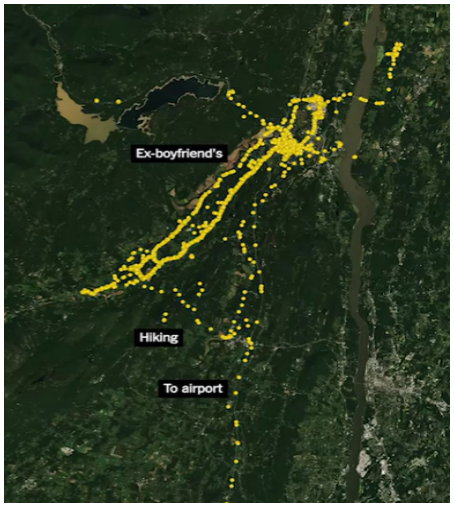

Figure 4 - This New York teacher was identifiable based on commercially available cellphone position data from her apps, many of them running in the background of her phone's operating system. (Source, The New York Times)

The Economics of Asymmetric Attacks

Defense professionals spent decades coming to grips with the consequences of economically beneficial asymmetric weapons. The missile revolution dominated the Cold War, as relatively cheap guided missiles became increasingly capable of destroying costly tanks, aircraft, and ships.[11] This, again, is nothing new. Just as gunpowder ended the age of edged weapons, machineguns unseated regiments of horse-mounted troops, and the advent of combat aircraft foretold the end of massive battleships, adversaries have always looked to new methods of creating a disproportionately large effect for relatively little cost. Terrorism emerged during

[10] Valentino-DeVries, Jennifer, Natasha Singer, Michael H. Keller, and Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *The New York Times,* December 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.
[11] Department of the Navy, "Lessons of the Falklands, Summary Report," *Government Printing Office,* February 1983, https://apps.dtic.mil/dtic/tr/fulltext/u2/a133333.pdf.

the "Pax Americana" as a cheap way for hostile nations to indirectly challenge the United States, with little opportunity cost yet disproportionately significant impact.

As near-peer adversaries struggle to compete with superior U.S. advantages, asymmetric attacks will increasingly offer alternatives to either costly economic competition or reckless direct conventional combat. A 2016 Congressional Budget Office report captured the direct and indirect costs of fielding U.S. expeditionary forces. The deployed Marine infantry battalion in the previous scenario costs the U.S. Government two years of a training-workup and deployment cycle, 1,500 unit members plus an additional 4,000 uniformed and civilian employees in the supporting establishment, and approximately $140 million dollars of direct annual investment plus another $600 million dollars of sunk costs.[12] When considering the economics, we should ask ourselves if a domestic attack against U.S. servicemember's families could be conducted for less than two years, 5,500 personnel, and $740 million dollars? The answer is, yes. In 2004, the Federal Bureau of Investigation (FBI) determined that the 9/11 terrorist attacks only cost the Al Qaeda terrorist network between

Figure 5 - A deployed Marine Battalion costs taxpayers $740 million dollars. Could adversaries neutralize this capability by attacking families at home? (Source, Sgt. Kyle Talbot, 5th Marine Expeditionary Brigade)

[12] The cost is likely much higher, as the report excluded research and development of new platforms and weapon systems, bases, facilities, construction costs, and long-term maintenance of the military establishment. (Congressional Budget Office, "The U.S. Military's Force Structure, A Primer," *Government Printing Office,* July 2016, https://www.cbo.gov/sites/default/files/114th-congress-2015-2016/reports/51535-fsprimerlite.pdf.)

$400,000 to $500,000 U.S. dollars.[13] Later, a Brookings Institution report determined the direct damages cost $100 billion, and the indirect cost to the economy and the wars in Iraq and Afghanistan cost an additional $6 trillion in what the report called, "the world's cheapest global game changer ever"[14] As long as the cost of preventing a $740 million dollar unit from reaching combat remains so astronomically low (not to mention the incalculable costs of morale, retention, readiness, and national prestige), it is only a matter of time before America's adversaries seize the opportunity to open a new chapter in fifth generation warfare that further blurs the lines between combatants and noncombatants.[15]

Figure 6 - 9/11 cost less than $500,000. (Source, Britannica)

Is the Threat Realistic?

It is always difficult to assess a threat that has not yet materialized. There is a historical basis for attacking families and civilians to disrupt military power. U.S. military support functions have been targeted as recently as the 2009 Fort Hood shooting, the 2013 Navy Yard shooting, and the 2019 Pensacola shooting, but not as directly or on such a scale as a coordinated attack by a near-peer state actor. By convention, nations have been restrained in their methods of warfare by international treaties, social conventions that dictate "fair play" in the conduct of war, fear of reciprocation, and the damage to national prestige or condemnation of the international community. Conventional constraints, however, may no longer be adequate to prevent the

[13] National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report: Executive Summary, Appendix A: The Financing of the 9/11 Plot," *Government Printing Office*, August 2004, https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_App.pdf.
[14] Riedel, Bruce, "Al Qaeda's 9/11 Obsession," *The Brookings Institution,* July 2011, https://www.brookings.edu/opinions/al-qaedas-911-obsession/.
[15] Qureshi, Dr. Waseem Ahmad, "Fourth- and Fifth- Generation Warfare: Technology and Perceptions," *San Diego International Law Journal, Vol 21, Issue 1,* Fall 2019, https://digital.sandiego.edu/cgi/viewcontent.cgi?article=1293&context=ilj.

targeted killing of military families as international institutions are increasingly threatened by global competition. The 2018 National Defense Strategy states the United States is "facing increased global disorder, characterized by a decline in the long-standing rules-based international order," and identifies Russia and China as "revisionist powers."[16] Further, both China and Russia have been condemned by the international community. Russia is the subject of multiple UN Resolutions calling for the withdrawal of Russian troops from Ukraine, and China continues to undermine human rights at the UN.[17] [18] Still, international pressure does not change the status quo. Transnational terrorist organizations, many with state sponsorship, have blatantly attacked civilian targets and killed countless women and children, yet western societies are unwilling to reciprocate in a similar fashion. When the old means of deterrence appear to be failing, it is time to develop new solutions to new problems.

The reality is that America's adversaries already use methods inconsistent with international norms. Russia continues to make headlines with targeted assassinations of political dissidents abroad.[19] [20] State sponsored hackers already target U.S. military families for low-level exploitation, such as one attack in 2015 when Russian hackers, posing as the Islamic State, sent threatening messages like, "We know everything about you, your husband, and your children and we're much closer than you can even imagine," to a military spouse while her husband was

[16] U.S. Secretary of Defense James Mattis, "Summary of the 2018 National Defense Strategy," *U.S. Department of Defense*, 2018.
[17] United Nations, "Resolutions Calling on Withdrawal of Forces from Crimea," *United Nations General Assembly, Seventy-Fifth Session, 36th Meeting,* December 2020, https://www.un.org/press/en/2020/ga12295.doc.htm.
[18] Richardson, Sophie, "Is China winning its fight against rights at the UN?," *Human Rights Watch,* December 2018, https://www.hrw.org/news/2018/12/12/china-winning-its-fight-against-rights-un.
[19] Groll, Elias, "A Brief History of Attempted Russian Assassinations by Poison," *Foreign Policy Journal,* March 2018, https://foreignpolicy.com/2018/03/09/a-brief-history-of-attempted-russian-assassinations-by-poison/.
[20] Berger, Miriam, and Adam Taylor, "Why Poison is the Weapon of Choice in Putin's Russia," *The Washington Post,* August 2020, https://www.washingtonpost.com/world/2020/08/21/why-poison-is-weapon-choice-putins-russia/.

deployed in the Middle East.[21] Why haven't we done anything to counter the threat already? Perhaps a lack of imagination prevents us from connecting the dots between the possible and the plausible until it is too late. As was discovered in the aftermath of the September 11th attacks, intelligence and military professionals, bureaucrats, and politicians alike fell victim to groupthink.[22] In the words of the 9/11 Commission Report, it may come as "a shock, [but] not a surprise."[23] Instead, let us reflect on the ominous words from the U.S. Secretary of Defense, "it is now undeniable that the *homeland is no longer a sanctuary*. America is a target."[24]

Figure 7- Children could be located with extreme precision, from when and where their parents dropped them off at school, to their path through the playground, and the location of their classroom. (Source, The New York Times)

Recommendations

The first step in securing this vulnerability is the further study by qualified professionals from military, law enforcement, counterterrorism, and domestic border protection under the umbrella of U.S. Northern Command's coordinating authority. Operational security (OPSEC) training is already offered by the Department of Defense to military families and is mandatory for servicemembers, but the increasing availability of data and complexity of attack vectors

[21] Volkman, Lori, "Opinion: Russian hackers attacked me and other military spouses. Why can't we sue?," *The Washington Post,* November 2019, https://www.washingtonpost.com/opinions/2019/11/19/russian-hackers-attacked-me-other-military-spouses-why-cant-we-sue/.
[22] Hamre, John, "A Better Way to Improve Intelligence," *The Washington Post,* August 2004, https://www.washingtonpost.com/archive/opinions/2004/08/09/a-better-way-to-improve-intelligence/30f772bd-24e0-4b93-a823-499b9c757e2c/.
[23] National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report: Executive Summary," *Government Printing Office*, August 2004, https://9-11commission.gov/report/.
[24] U.S. Secretary of Defense James Mattis, "Summary of the 2018 National Defense Strategy," *U.S. Department of Defense*, 2018.

require a ground-up review of current and future cyber-protection and OPSEC training, as well as its effectiveness. Additionally, a separate threat working group with FBI and Homeland Security should make further recommendations to the Department of Defense for improved protective measures.

There may be additional legislative measures necessary to further mitigate foreign risks to military families. Social media platforms should be required to add additional layers of protection for certain types of activities, like military community group sites and events. Increased scrutiny of new members and restrictions on setting up "unofficial" group sites would prevent unintentional leaks from community members. The further protection of open-source information like unit webpages behind login and password access might pose a minor inconvenience for extended family members who want to know about their servicemember's unit, but offer a reasonable tradeoff between cost and risk mitigation.

Finally, the geographic concentration of military families around large military bases, installations, and fleet concentration areas presents one of the most lucrative, target-rich environments for hostile actors. Initially, U.S. Cyber Command's mission could be extended to protect U.S. servicemembers' families in the cyber domain, especially in military concentration areas. Further, it may be necessary to federalize off-base law enforcement in these areas to ensure they have access to military and national-level intelligence, sufficient interagency coordination, jurisdiction, and federal funding for resources beyond state and local capabilities.

NOTES

Figure 1. "U.S. Defense Spending Compared to Other Countries," *Peter G. Peterson Foundation,* May 2020, https://www.pgpf.org/chart-archive/0053_defense-comparison.

Figure 2. "UN report: 188 civilian casualties in eastern Ukraine over three months," *Human Rights Centre ZMINA,* September 2016, https://zmina.info/en/news-en/za_3_misjaci_na_skhodi_ukrajini_postrazhdali_188_osib__dopovid_oon-3/.

Figure 3. "11th Marine Expeditionary Unit: Leadership," *U.S. Marine Corps official website,* 2021, https://www.11thmeu.marines.mil/.

Figure 4. Valentino-DeVries, Jennifer, Natasha Singer, Michael H. Keller, and Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *The New York Times,* December 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

Figure 5. Talbot, Sgt. Kyle, "26th Marine Expeditionary Unit Trains on Saudi Arabian Islands," *U.S. Marine Corps official website,* April 2020, https://www.marines.mil/News/News-Display/Article/2347211/26th-marine-expeditionary-unit-trains-on-saudi-arabian-islands/.

Figure 6. Bergen, Peter L., "September 11 Attacks," *Britannica,* September 2020, https://www.britannica.com/event/September-11-attacks.

Figure 7. Valentino-DeVries, Jennifer, Natasha Singer, Michael H. Keller, and Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *The New York Times,* December 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

BIBLIOGRAPHY

"Afghanistan: Targeted Killings of Civilians Escalate," *Human Rights Watch,* March 2021, https://www.hrw.org/news/2021/03/16/afghanistan-targeted-killings-civilians-escalate#.

Berger, Miriam, and Adam Taylor, "Why Poison is the Weapon of Choice in Putin's Russia," *The Washington Post,* August 2020, https://www.washingtonpost.com/world/2020/08/21/why-poison-is-weapon-choice-putins-russia/.

Bouckaert, Peter, "War Crimes in Chechnya and the Response of the West: Testimony Before the Senate Committee on Foreign Relations," *Human Rights Watch,* February 2000, https://www.hrw.org/news/2000/02/29/war-crimes-chechnya-and-response-west.

Congressional Budget Office, "The U.S. Military's Force Structure, A Primer," *Government Printing Office,* July 2016, https://www.cbo.gov/sites/default/files/114th-congress-2015-2016/reports/51535-fsprimerlite.pdf.

Department of the Navy, "Lessons of the Falklands, Summary Report," *Government Printing Office,* February 1983, https://apps.dtic.mil/dtic/tr/fulltext/u2/a133333.pdf.

Elder, Gregory, "Intelligence in War: It Can Be Decisive," *U.S. Central Intelligence Agency, Studies in Intelligence, Vol 50, No 2,* 2006, https://apps.dtic.mil/sti/pdfs/ADA497904.pdf.

Groll, Elias, "A Brief History of Attempted Russian Assassinations by Poison," *Foreign Policy Journal,* March 2018, https://foreignpolicy.com/2018/03/09/a-brief-history-of-attempted-russian-assassinations-by-poison/.

Hamre, John, "A Better Way to Improve Intelligence," *The Washington Post,* August 2004, https://www.washingtonpost.com/archive/opinions/2004/08/09/a-better-way-to-improve-intelligence/30f772bd-24e0-4b93-a823-499b9c757e2c/.

National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report: Executive Summary," *Government Printing Office*, August 2004, https://9-11commission.gov/report/.

National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report: Executive Summary, Appendix A: The Financing of the 9/11 Plot," *Government Printing Office*, August 2004, https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_App.pdf.

O'Hanlon, Michael E., "What the Pentagon's new report on China means for US strategy – including on Taiwan," *The Brookings Institution,* September 2020, https://www.brookings.edu/blog/order-from-chaos/2020/09/04/what-the-pentagons-new-report-on-china-means-for-u-s-strategy-including-on-taiwan/.

Qureshi, Dr. Waseem Ahmad, "Fourth- and Fifth- Generation Warfare: Technology and Perceptions," *San Diego International Law Journal, Vol 21, Issue 1,* Fall 2019, https://digital.sandiego.edu/cgi/viewcontent.cgi?article=1293&context=ilj.

Richardson, Sophie, "Is China winning its fight against rights at the UN?," *Human Rights Watch,* December 2018, https://www.hrw.org/news/2018/12/12/china-winning-its-fight-against-rights-un.

Riedel, Bruce, "Al Qaeda's 9/11 Obsession," *The Brookings Institution,* July 2011, https://www.brookings.edu/opinions/al-qaedas-911-obsession/.

Roug, Louise, "Targeted Killings Surge in Baghdad," *Los Angeles Times,* May 2006, https://www.latimes.com/archives/la-xpm-2006-may-07-fg-civilians7-story.html.

United Nations, "Pillay alarmed by killing of civilians in Ukraine," *United Nations Human Rights, Office of the High Commissioner,* August 2014, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14975.

United Nations, "Resolutions Calling on Withdrawal of Forces from Crimea," *United Nations General Assembly, Seventy-Fifth Session, 36th Meeting,* December 2020, https://www.un.org/press/en/2020/ga12295.doc.htm.

"U.S. Defense Spending Compared to Other Countries," *Peter G. Peterson Foundation,* May 2020, https://www.pgpf.org/chart-archive/0053_defense-comparison.

U.S. Secretary of Defense James Mattis, "Summary of the 2018 National Defense Strategy," *U.S. Department of Defense*, 2018.

Valentino-DeVries, Jennifer, Natasha Singer, Michael H. Keller, and Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *The New York Times,* December 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

Vergun, David, "Spacecom Aims to Ensure Space Domain is Protected, General Says," *U.S. Department of Defense: DOD News,* May 2021, https://www.defense.gov/Explore/News/Article/Article/2593617/spacecom-aims-to-ensure-space-domain-is-protected-general-says/.

Volkman, Lori, "Opinion: Russian hackers attacked me and other military spouses. Why can't we sue?," *The Washington Post,* November 2019, https://www.washingtonpost.com/opinions/2019/11/19/russian-hackers-attacked-me-other-military-spouses-why-cant-we-sue/.