Soft Networks: Protecting an Achilles Heel of American Influence

By Steve Miska, Rebecca Asch, and Samuel Romano

Pacific Council
ON INTERNATIONAL POLICY

Purpose

The purpose of the research and policy effort is to strengthen U.S. national security by infusing resilience into soft networks through robust policy options and operational practices. This white paper can be used as a primer to:

- Facilitate interagency policy development to protect soft networks
- Promote policy and doctrinal development at the department/agency level
- Conduct further research

The project to Strategically Protect Soft Networks[1] exists as a partnership of nonprofits, academic institutions, veterans, and diplomats. In 2018 the project benefited from a grant from the Smith Richardson Foundation. Learn more about SPSN at protectingsoftnetworks.org

Definition

Soft networks refer to indigenous partners in diplomatic, military, intelligence, and law enforcement operations, and often include interpreters, local business contractors, politicians, teachers, intellectuals, religious leaders, and others deemed vital to U.S. national interests, as well as their families. These local national partners are integral to achieve United States national security interests and provide invaluable support to American diplomatic and military efforts in conflict zones—often in spite of tremendous danger from adversaries.

Background

Threats against soft networks represent a viable impediment to U.S. foreign policy objectives. More than merely supporting operations, soft networks are integral to successful missions abroad. Insufficient protection of soft networks demonstrably decreases the efficiency of counterinsurgency operations for the U.S. military and diminishes U.S. military engagement with the population. Critical indigenous partners enable intelligence operations and law enforcement investigations abroad, and diplomats rely heavily on local partners for cultural understanding. Failing to protect soft networks weakens local national confidence in ongoing U.S. military and diplomatic efforts, damages host-nation military relationships with U.S. forces, and dilutes U.S. narratives regarding objectives in conflict zones.

After the onset of the wars in Iraq and Afghanistan, the United States required protective measures to ensure a collaborative effort between U.S. forces and local national allies. In both countries, adversaries like the Taliban, al Qaeda, Shia militias, and Sunni insurgents often sought to deliver retribution against those who supported Coalition Forces and violently attacked interpreters and other local national support staff. In some cases, indigenous government officials even aided or ignored insurgent and militia attacks against U.S. local national allies. As a result of these

[1] SPSN exists as a partnership of nonprofits, academic institutions, veterans, and diplomats. In 2018 the project benefited from a grant from the Smith Richardson Foundation. As part of Phase III of SPSN's grant proposal, the project is committed to publishing its research results in a white paper listing all identified best practices. This white paper provides an overview of SPSN's research results, particularly with regard to best practices sourced from non-governmental and government sources and provides recommendations for policy implementation, as well as, next steps for continued research.

hindrances and the lack of active protective measures, local national allies often became easy targets for U.S. adversaries.

Currently, methods for protecting soft networks are ad-hoc and largely ineffective. Interpreters and others adopt identity protection practices that include using aliases, alibis, and surreptitiously commuting to embassies, posts, and bases. Local nationals are compelled to lie to their family and friends about their work, even after their term of service has ended. These ad-hoc measures offer some amount of protection, but are neither systemic nor sustainable. Moreover, ad-hoc measures fail to address developing cyber threats or ways that service-members can protect partner identities. While Congress passed the Special Immigrant Visa (SIV) in 2006 to protect at-risk local national partners, the SIV has been a necessary but insufficient policy option to insulate soft networks.

The Special Immigrant Visa is designed to offer U.S. immigration visas to Iraqi and Afghan nationals who worked on behalf of the U.S. government. However, the process was long and complicated, and only a small portion of those who qualified for visas were able to successfully immigrate to the U.S. Despite active engagements in conflict zones around the globe (Syria, Yemen, Somalia, etc.), the SIV only remains active for Afghan local nationals, with Congress authorizing 4,000 visas for 2019[2]. As the U.S. draws down in Afghanistan, the number of SIVs approved has dwindled, even though Congress authorizes additional visas annually. Despite the bureaucratic shortcomings of the SIV, it remains a powerful tool for extracting individuals who are out of options. A failure to more actively protect soft networks will continue to endanger local national partners, and, moreover, will endanger current and future U.S. military and diplomatic engagement around the world.

Following an analysis, this paper surveys potential policy options and practical options to better insulate soft networks. First, we highlight non-military actor (such as NGOs) interaction with local national partners and how those practices can be incorporated into U.S. policy. Second, we survey cyber security weaknesses to soft networks, and potential practices the U.S. can incorporate to protect local national partner digital presence from adversaries. Third, we review current defense contracting laws and practices to identify gaps in current contracting policy. Building on the analysis, this paper will then offer recommendations and possible next steps for research and policy development.

Analysis

1. Non-Military Best Practices

Efforts to protect local national partners in conflict zones and other insecure environments continue to vary between international actors, often depending on actor capabilities and roles. Non-governmental organizations (NGOs) often conduct operations in conjunction with local partners and face similar issues regarding the protection of important networks and vulnerable individuals. For example, in one study, 69 percent of attacks against NGO staff targeted local national staff.[2]

[2] H.R. Res. 31, Section 7076, 116 Cong. (2019) (enacted) - Consolidated Appropriations Act 2019
[2] Fast, Larissa. "Characteristics, Context and Risk: NGO Insecurity in Conflict Zones." Disasters31, no. 2 (2007): 130-54. www.doi:10.1111/j.1467-7717.2007.01001.x.

Moreover, local national staff were 50 percent less likely to receive training to protect themselves from belligerents,[3] and faced visible disparities between security precautions taken to protect themselves compared to precautions taken to protect international staff.[4]

In light of similar necessity for NGOs to protect soft networks, SPSN conducted research regarding protection methods that could apply to U.S. military and diplomatic forces abroad. This section of research separates best practices into a three-pronged framework consisting of: (1) pre-conflict practices, (2) conflict practices, and (3) international legal classifications.[5]

1.1. *Pre-Conflict Practices*

Many non-military actors, including NGO staff and peacekeeping forces, approach conflict environments with ingrained assumptions, particularly regarding common practices and narratives. Non-military actors typically resort to assumptions and transplanted practices as a result of time constraints, which prevent the preparation of tailored practices, and/or "cognitive overload," in which an actor must prepare for multiple tasks at once.[6] As a result, approaching a new environment using assumptions and common practices allows practitioners to transplant established methods between different environments, easing transition processes and training requirements. Yet, these approaches also lead to critical misunderstandings regarding local circumstances and allow practitioners to ignore the detriment transplanted practices can have in dangerous environments.

Similarly, soft networks inevitably suffer from U.S. military and diplomatic failure to factor local national partner importance into planning. The build-up to any conflict involves both time constraints and cognitive overload, and in the case of many conflicts, military and diplomatic leaders have repeatedly missed important considerations regarding soft network insulation. Foreign service and military officers generally conduct careful evaluation of new environments, yet, organizational turnover leads to inexperienced planners, particularly in the military. Training and education on soft networks would cause practitioners to evaluate new environments and factor soft network resilience in planning processes and overall mission accomplishment.

Threat assessments are one of the methods utilized by non-military actors to understand a hostile environment prior to deployment. These assessments are integral to overall preparedness, and outline the presence and potential effects of local tensions, insurgent and military forces, and levels of crime.[7] Similarly, the non-military sector has developed a categorization system that segments potential threats by the presence of "ambient danger," or threats resulting from the overall level of danger in an environment, and "situational danger," or the presence of targeted threats to individuals or groups based on affiliation.[8] Adversaries intentionally target American soft

---

[3] Ibid.
[4] InterAction. "The Security of National Staff: Towards Good Practices" *InterAction Report* (2001).
[5] It is important to emphasize that these are not separate recommendations, each of which should be independently implemented. Rather, examples of best practices from non-military sectors should be taken as a symbiotic framework, each of which are necessary to benefit the others.
[6] Autesserre, Séverine. "International Peacebuilding and Local Success: Assumptions and Effectiveness." *International Studies Review* (2017).
[7] InterAction. "The Security of National Staff: Towards Good Practices" *InterAction Report* (2001).
[8] Fast, Larissa. "Characteristics, Context and Risk: NGO Insecurity in Confict Zones." Disasters31, no. 2 (2007): 130-54. www.doi:10.1111/j.1467-7717.2007.01001.x.

networks, thereby categorizing the majority of threats in the situational danger bucket of the framework.

Integrating threats assessments that analyze local circumstances in hostile foreign environments, as well as the ambient/situational danger method in conflict planning would enable the U.S. to better understand potential threats in new conflicts and mitigate risks. Moreover, this knowledge would allow the U.S. to more effectively insulate its soft networks prior to deployment by understanding the threats faced by local national partners and adapting insulation methods to fit given situations.

1.2. *Conflict Practices*

In addition to best practices that should be established prior to a U.S. military and diplomatic deployment to foreign environments, practitioners would benefit from non-military best practices for securing local national assets during conflict.

The NGO community has often failed to adequately protect at-risk local national staff members. In response to these dangers, NGOs have attempted to develop best practices to more effectively protect local national staff. NGOs have largely recommended a diverse "toolkit" from which field-based practices can be refined and utilized based on given circumstances. Yet, NGOs also recognize the effectiveness of dictating certain policies, via a top-down policy structure, for organizations in hostile environments.[9] Many of these policies could be quickly adapted to fit the U.S. military and diplomatic structure and would greatly aid soft network insulation.

NGOs recommend including local partner participation in evaluating and structuring insulation methods and training, and contributing to decision-making on key issues concerning local national staff security.[10] Furthermore, NGOs recommend continuing threat assessments to evaluate and refine field practices based on the security situations and necessities of local partners.[11] Local partners, particularly those likely to face high levels of violence, can be given security orientation and training regarding the risks they may face, briefed on potential insulation options and flight plans (including identity protection measures), and informed as to how they can safely and promptly communicate concerns regarding their risk status.[12] Integrating these measures into existing military doctrine by developing standard operating procedures that delineate how threats and violence against local partners are reported, received, investigated, and addressed[13] would likely bolster soft network insulation policies.

Finally, while non-military best practices are meant to proactively insulate partners, preventing more extreme measures like relocation, NGOs recognize the likelihood that some local national partners will require relocation. Yet, in contrast to the SIV (which requires relocation to the U.S.), NGOs have advocated against extreme relocation, understanding that relocation to the United States, or a similar host-country, can often be jarring for local national partners, as well as timely, costly, and dangerous. In the event of a serious deterioration in the security situation of a

[9] InterAction. "The Security of National Staff: Towards Good Practices" *InterAction Report* (2001). 3.
[10] Ibid.
[11] Ibid. 4, 12.
[12] Ibid. 4-5.
[13] Dalton et al. "Civilians and "By, With, and Through." *CSIS* (2018). 7.

local partner, NGOs recommend local and regional relocation to efficiently relocate the partner, and allow local national partners to continue their quality of life with minimal disruption.[14] Any policy to insulate soft networks would be wise to follow suit, only resorting to extreme relocation measures in situations where local partners face dire risk and local relocation appears insufficient. Yet, we emphasize that, due to the potential of situations in which local and regional relocation is insufficient, the U.S. must ensure that the SIV is not eliminated and remains as a last resort to aid at-risk partners.

1.3. *International Legal Classifications*

In addition to practical non-military recommendations, SPSN research has identified legal practices that would benefit soft network protection, particularly related to the civilian/combatant classification under international law.

Under international law, individuals in conflict zones are classified as either civilians or combatants and afforded legal protections based on their classification. Soft networks occupy a similarly difficult position to classify. While soft networks are rarely armed, local national partners often accompany active combat units and inherit the dangers of combat. As such, classifying soft networks as civilians under international law would ignore their role in the U.S. military and diplomatic structure. As a result of being generally unarmed, soft networks forego combatant classification and the afforded legal protections. U.S. government lawyers could greatly assist soft network insulation by identifying legal classifications to better protect local national partners, particularly as a consequence of combat unit affiliation.

2. Best Practices for Cyber Identity Protection[15]

In December 2014, after monitoring service member social media accounts to identify potential enemies, [16] the hacking division of the Islamic State in Iraq and Syria (ISIS) released a hit list of American service members, including their names, addresses, family members and photos.[17] As social media use continues to proliferate worldwide, its use by adversaries as an intelligence source will increase. While we continue to research this phenomenon with regard to soft networks, the potentially detrimental effects of social media have been demonstrated in parallel situations. Domestically, the FBI has highlighted criminal use of social media to identify and target officers,[18] and, moreover, has received multiple reports of witness intimidation through

---

[14] InterAction. "The Security of National Staff: Towards Good Practices" *InterAction Report* (2001). 5, 10.
[15] Some cyber best practices come from U.S. government recommendations through participation in interviews and round table discussions.
[16] Ross, Brian, and James Gordon Meek. "ISIS Threat at Home: FBI Warns US Military About Social Media Vulnerabilities." ABC News. December 01, 2014. https://abcnews.go.com/International/isis-threat-home-fbi-warns-us-military-social/story?id=27270662.
[17] "ISIS Targeting Military Members Via Social Media." University of Texas at Austin, Center for Identity. https://identity.utexas.edu/id-perspectives/isis-targeting-military-members-via-social-media.
[18] "Social Media and Law Enforcement." FBI. November 01, 2012. https://leb.fbi.gov/articles/featured-articles/social-media-and-law-enforcement.

Facebook[19] and Instagram.[20] Anecdotally, SPSN has received reports of the Taliban torturing and killing former interpreters and posting grisly videos on Facebook to intimidate other interpreters.[21] The use of social media to target law enforcement and private citizens who aid law enforcement operations sets a dangerous precedent for future use against local national partners who aid U.S. military and diplomatic forces abroad.

Given the need for more research to quantify threats to soft networks, SPSN believes that implementing cyber security best practices could greatly enhance identity protection. Future research may yield insight to the extent of adversary targeting on social media and other cyber areas.

2.1. *Pre-Conflict Practices*

Military and diplomatic forces should institute a program that integrates cyber hardware, software, and technology security. Prior to insertion, U.S. personnel should identify a country's cyber footprint, its electronic landscape, and its cultural effect on online presences (such as social media and telecommunications). Further, clear protocols should be established regarding the use of foreign or local technology in conflict zones and the effect this use may have on local partners, particularly considering the benefit of adapting distributed technology to local norms in order to prevent identification by belligerents. Finally, all digital connections (such as state infrastructure, satellite, or LAN/WAN) should be evaluated prior to a conflict for dangers of potentially exposing local partner identities.

2.2. *In-Country Practices*

Following insertion, US military forces and diplomats should ensure their communication tools, such as laptops, tablets, phones, GPS, and radios, protect local partner identities. Devices should be adapted to local norms, and hardware should include encryption, two-factor authentication, and log-in authentication. Moreover, in cases where a local national partner is searched, or their devices are otherwise compromised, all devices supplied by U.S. forces to local nationals should include the ability to be wiped remotely. So too, local national partners should be encouraged to use multiple SIM cards, so personal information and connections to the U.S. government are obscured if their cellular device is lost, stolen, or otherwise removed from their person.

These practices, while far from fully countering the cyber threat to our soft networks, would represent a tangible step toward effectively protecting local national partners in the age of widespread technological use. However, there is certainly more research that needs to be done on this front, and we expect cybersecurity research to be one of SPSN's major 'next steps' going forward.

3. Contracting Practices

[19] "Witness Intimidation on Social Media: Law Enforcement's Growing Challenge." NBCNews.com. November 15, 2013. https://www.nbcnews.com/news/us-news/witness-intimidation-social-media-law-enforcements-growing-challenge-flna2D11599928.

[20] "Violent Crime Witnesses Targeted on Instagram." NBCNews.com. November 08, 2013. https://www.nbcnews.com/technology/violent-crime-witnesses-targeted-instagram-8C11565158.

[21] For example, watch Vice News story by Ben Anderson at https://www.youtube.com/watch?v=k7k1XJcDpV4

3.1. *Reorienting Contracting Processes and Protections*

Government contractors, both American and foreign hires, have become ubiquitous as U.S. military and diplomatic augmentees to secure national security interests abroad. According to a 2008 Congressional Budget Report, nearly 70,000 local nationals worked on American contracts in Iraq,[22] and, as recently as October of 2018, over 3,000 local national contractors were working on Department of Defense contracts in Afghanistan.[23] Most local nationals who serve as interpreters or provide other services on behalf of the U.S. government are hired by a subcontractor who works on behalf of a government contracting firm. As such, it is vital to recognize the importance of addressing contracting as a system through which local national allies interact with the U.S. government. By and large, contracting law and policies as they apply to local nationals have been overly sweeping and tend to ignore the specific security needs of this group.

Contracted local nationals are employed by the U.S. government through a complex chain of command wherein local nationals are directly employed by a subcontractor, which is in turn employed by a prime contractor, which itself is responsible to the U.S. government. This complex chain of responsibility can often lead to oversights and loopholes that threaten the safety of local nationals and service members alike. As this section outlines, some of these oversights have resulted in very real dangers for local national contractors.

3.2. *New Model for Protection Based on CTIP*

Local nationals are not only contractors for the U.S. government, but they are also an especially vulnerable population due to the high likelihood of threats against them from nefarious actors. Given their unique vulnerability and the U.S. government's heavy reliance on them, local national contractors should be afforded protections within the Federal Acquisition Regulation (FAR)[24] and the Defense Federal Acquisition Regulation System (DFARS). Yet, the U.S. government does not currently have a system in place for protecting them as a uniquely vulnerable population.

In other contexts, the U.S. has enacted policy to protect local nationals. For example, Combatting Human Trafficking in Persons (CTIP) establishes offices throughout the government to protect vulnerable employees from human trafficking abuses in conflict zones. These protections are overseen by various government program management offices (PMOs). CTIP offices provide training for federal employees who interact with at-risk populations to ensure that they can identify human trafficking, educate local national subcontractors on their rights as U.S. subcontractors, and train local national partners to identify when those rights are being violated, or worse, when they are being trafficked. CTIP PMO affiliates also provide on-the-ground oversight measures

---

[22] United States. Congressional Budget Office. *Contractors' Support of U.S. Operations in Iraq.*By Daniel Frisk, R. D. Trunkey, Adam Talaber, Adebayo Adedeji, Victoria Liu, Robert Dennis, Theresa Gullo, Frank Sammartino, Robert Murphy, and Jennifer Elsea. August 2008. https://www.cbo.gov/sites/default/files/110th-congress-2007-2008/reports/08-12-iraqcontractors.pdf.

[23] United States. Department of Defense. CENTCOM. *CONTRACTOR SUPPORT OF U.S. OPERATIONS IN THE USCENTCOM AREA OF RESPONSIBILITY* .October 2018. https://www.acq.osd.mil/log/ps/.CENTCOM_reports.html/5A_October_2018.pdf.

[24] The Federal Acquisition Regulation serves as a guide for federal contracting across government, not just for defense.

(including deploying inspectors and observers) to inspect working conditions for third-country nationals and ensure they aren't exploited.

The CTIP model is one that could be emulated in the effort to protect soft networks. This whole-of-government model of systemic protective measures is exactly what is needed to protect soft networks in the long-term. Protecting local nationals stands to benefit U.S. national security interests, possibly more so than the benefits of combating human trafficking. Departments across government should therefore take the plight of soft networks as seriously as they do human trafficking and implement similar protective measures.

3.3. *Contract Language*

Clear contract language guaranteeing subcontractor safety is vital in an environment as complex and unstable as a warzone. This necessity is especially true for local national subcontractors, who depend on their contractor and on the U.S. government to ensure that they are protected from threats stemming from their affiliation with the United States. However, local national partner contracts are often vague and fail to address tangible employee safety concerns. As a result, local national contractors are left without legal recourse if they are harmed or killed as a result of U.S. government affiliation.

Given the need for more research in this area, SPSN has been unable to quantify the scope of the threat to local nationals. However, one leaked document to T. Christian Miller, a *ProPublica*[25] journalist, indicates that in one year 360 interpreters were killed with another 1,200 wounded from one contracting firm.[26] One contract between an Iraqi translator and a major contractor from 2008[27] illustrates the shortcomings of legal language in local national contracts. The one-year contract example is only five pages long with both English and Arabic translations included. Most of the contract outlines punitive action that would befall the translator if he were to break protocol or leak sensitive information. Only at the contract's conclusion does the document ask the subcontractor to assume any risks of personal injury or death that result from performance of his duties and stipulates in all-caps. [27]

> THE SUBCONTRACTOR AGREES TO RELEASE [contractor] AND THE UNITED STATES GOVERNMENT FROM ANY AND ALL LIABILITY, HOWEVER CAUSED, WHETHER DIRECT OR INDIRECT, RESULTING FROM ANY PERSONAL INJURY OR LOSS, INCLUDING DEATH, WHICH MAY BE SUSTAINED.

In consultation with legal professionals, it appears that this contract was indeed legal, as the contract later acknowledges coverage under the Defense Base Act.[28] Nevertheless, on first read it seems that the contract is in violation of the DBA, given that it states in all-caps that the contracting firm is not liable for death or injury prior to acknowledging coverage under the DBA. Moreover,

---

[25] *ProPublica* is an American nonprofit organization based in New York City. It is a nonprofit newsroom that aims to produce investigative journalism in the public interest.

[26] T. Christian Miller compiled a spreadsheet of contractor deaths recorded by L3 Systems in May 2008. The data show that 360 Iraqi translators and interpreters were killed while serving under an L3 contract, and 1,200 were wounded. The spreadsheet can be found here: https://www.propublica.org/article/chart-iraqi-translators-a-casualty-list

[27] A contract was volunteered to the project by a former male local national contractor.

[28] "DBA Information." United States Department of Labor. https://www.dol.gov/owcp/dlhwc/explainingdba.htm#2

the contract does not explicitly review what constitutes coverage under the DBA, presumes that the subcontractor understands how they are covered, how to access coverage, and when coverage ends. This language is objectively vague, and likely even more unclear to an individual who isn't well versed in American law or the DBA.

Beyond its unclear language, the contract requires an untrained, unprotected individual to operate in combat zones, and strips them of the ability to take legal action against their employer. In order to effectively protect soft networks, the U.S. must ensure that future contracts between local national partners and defense contractors are straightforward and do not include language that may suggest that they are left out to dry by the U.S. government.

Under the Defense Base Act, non-American civilian contractors are included under the insurance requirement. There are certain 'blanket waiver' countries, wherein the contractor does not need to secure insurance for their employees if they are foreign nationals of that country — however, neither Iraq nor Afghanistan are on that list.[29] Waivers can also be obtained if the employee already has insurance that covers workplace injury or death. In this instance the translator was unaware of his rights for protection under the DBA and signed away his right to hold his employer accountable for his safety.

Policy Recommendations

Current policy solutions for protecting soft networks fall short of investing in resilient, viable soft networks. Creating a system of policies that will appropriately protect these individuals will require a persistent and concerted effort. With enough political will, efforts toward ensuring the security of our local national partners will benefit long-term national security interests.

The following section puts forth several recommendations and best practices for policymakers that would better protect soft networks. These recommendations are based on research, interviews, and prior efforts to insulate soft networks. As institutional partners continue to remind Congress and the public of the importance of soft networks, these recommendations and best practices represent a toolkit for effectively securing soft networks.

1. Assign Responsibility

   In any organization, a leader owns responsibility for the mission. Protecting soft networks, as a component of mission success, is no different. When a leader is tasked with ensuring that local national contractors aren't being threatened or abused, the contractors are more likely to remain safe and contribute to mission success. The CTIP program provides a useful example.

   Ultimately, the National Security Council (NSC) should act as an arbiter of a policy development process.[26] Ideally, an NSC Senior Director would own the process with stakeholder agencies like DoD and State selecting the appropriate departmental leads like

[29] USAID. *Guidelines for DBA Coverage for Direct and Host Country Contracts*. June 2007. https://www.usaid.gov/sites/default/files/documents/1868/302sap.pdf

[26] See Appendix II for an example of a policy development process through a National Security Study Directive.

the Undersecretary of Defense for Intelligence, for example. Each department or agency would provide representatives to shepherd policy development and ultimately ensure that diplomats and commanders in the field understand strategic risks and recommend policy prescriptions to mitigate the threats.

The Defense Contracting Management Agency (DCMA) should also exercise greater oversight over contracts between American companies and local nationals to ensure that all laws are being followed. Contracting language needs to be consistent with current law so that vulnerable populations aren't denied protections consistent with U.S. law.

2. Develop Policy & Doctrine

Appendix II provides a model policy makers could adopt for a comprehensive policy development process. Current practices enacted to protect soft networks are based on ad-hoc, bottom up initiatives, many times stemming from local nationals themselves. These measures do not consider the fluid and dangerous situations that local nationals are often exposed to and fail to integrate policy measures that could proactively protect local national partners. In short, current efforts are often "too little, too late." Policy that prioritizes identity protection and local/temporal relocation methods would expand the practitioner's toolkit. The ultimate goal of the recommended policy development process is an array of tools available to practitioners in the field to effectively insulate soft networks abroad.

In order to proactively protect local national partners, policymakers should develop the means to insulate soft networks prior to deployment, such as threat assessments that provide accurate information to evaluate local partner risk. Moreover, threat assessments should be used to inform identity protection and relocation policy for at-risk local nationals. While fully removing a local partner and their family is sometimes appropriate, oftentimes a threatened local partner can find safety by relocating to an area nearby, potentially on a temporal basis depending on the specific case. Doing so would relieve the pressure on the SIV system, allow local partners additional control over their own affairs, and create a wider network of viable solutions in threat situations.

Furthermore, SPSN recommends that the U.S. policymaking community make an effort to definitively classify local national partners as combatants, civilians, or some other special legal category. By existing in the grey area between civilian and combatant, soft networks are not afforded the protections and advantages of either classification. Thus, future legal research and analysis should explore how to provide better legal protections.

3. Implement Education & Training

Local nationals serving in fields of combat (including interpreters) are required to undergo basic law-of-war training, and to enroll in SPOT (synchronized pre-deployment and operational tracker) to train and track contracted employees for the U.S. government. However, this training does not focus on identity protection or safety precautions that are specific to local nationals. The SPOT training in particular is more focused on tracking individuals in theatre than on training and protecting them. Training should also incorporate cyber security within the overall identity protection umbrella.

SPSN recommends that local nationals be afforded training that focuses on identity protection. This training should also be made available to deploying units and government personnel who interact with local nationals. A training program of this nature would emphasize the specific needs of local nationals and would improve their ability to maintain their own safety. When conditions warrant, local nationals should contribute to training development as highlighted in NGO best practices.

We also recommend that issues relating to protecting soft networks be integrated into wargames and tabletop training for deploying government personnel. Wargaming is a vital tool by which military leaders (and is gaining wider acceptance for other government practitioners) prepare and test strategies and requires participants to keep a number of varying components in mind in order to effectively implement a strategy. Keeping soft networks safe is an important element in an effective and sustainable strategy, and it should be reflected in exercises. If successful, this 'next step' will lead to budding senior service-members that are more aware and thoughtful about how they interact with their soft networks. Moreover, integrating soft network protection as a component in tabletop exercises would test proposed best practices before they are implemented on the battlefield.

4. Expand the Special Immigrant Visa (SIV)

The SIV is currently the best in-practice tool for bringing former contracted local nationals to the U.S. However, the Iraq SIV ceased accepting new applications in 2014, resulting in about 60,000 Iraqis awaiting processing as of 2018.[27] The Afghan SIV, while still technically active, only allocated 4,000 SIVs in 2019[28] for former Afghan contractors—a fraction of the amount needed. With a potential drawdown in Afghanistan, there will be more Afghans who will need to escape violence due to U.S. affiliation.

Importantly, many interpreters who arrived in the United States via the SIV have become a vital talent pool for government contracting firms. Some have enlisted in the U.S. Army or Marine Corps, deploying back to combat, serving in vital training functions, and other capacities. Some SIV recipients continue to serve with high security clearances in the

[27] How the Trump Administration's Executive Orders on Refugees Harm Our Iraqi Wartime Allies." Human Rights First, September 19, 2018. https://www.humanrightsfirst.org/resource/how-trump-administrations-executive-orders-refugees-harm-our-iraqi-wartime-allies

[28] H.R. Res. 21, Section 7076, 116 Cong. (2019) (enacted) – Consolidated Appropriations Act 2019

defense contracting community conducting important missions like counter-ISIS messaging on social media and other platforms.

Though there are certainly many problems with the SIV (not limited to its long processing time and the difficulty for SIV recipients to migrate and adjust to their new home), it remains an effective tool that needs to be kept alive, ideally as an option of last resort. SPSN partners have worked tirelessly to advocate on Capitol Hill for maintaining the SIV and spreading public awareness regarding the importance of this visa. We support their efforts and recommend that policymakers commit to maintaining and increasing the number of available SIVs for Afghans. Congress should also authorize SIVs in any active conflict where diplomats and military personnel rely on soft networks.

Next Steps

Protecting soft networks requires time, effort, and resources, but success is vital to U.S. national security interests abroad. In addition to research and recommendations compiled above, we have outlined a number of short and long-term 'next steps' we aim to complete.

1. Further Research

1.1. *Catalogue Soft Network Attacks*: Pursue additional research into attacks, injuries, and deaths of local national partners. Failure to assess the strategic scope of threats to soft networks hinders policymaker ability to prioritize soft network insulation measures. Moreover, every step of the policy development process would benefit from access to this data, as a more accurate understanding of the threat to our soft networks, particularly with regard to which local national partners are most at risk (i.e. translators, business contractors, etc.). This information would further illuminate the necessity to protect soft networks and allow the U.S. to assess the scope of threats and effectively prioritize policy efforts.

1.2. *International Legal Protections*: While we have included preliminary research on international legal classifications of soft networks, integrating international legal protections into future soft network insulation measures, particularly related to local national partner classification, would aid soft network insulation geopolitically.

1.3. *Contracting Research:* The DFARS and other contracting guidelines for the government are complicated, vast, and ever-changing. The project will continue to monitor contracting reforms and laws that are pertinent to Soft Network research and will investigate provisions that appear to be detrimental to protecting local national partners.

1.4. *Cybersecurity Protection*: Cybersecurity concerns continue to develop throughout the U.S. government. As social media and technology proliferate in many conflict zones, further research is required to study the effects of cybersecurity protection on insulating local national partners.

1.5. *Develop Partnerships with Domestic Policy Development Organizations*: Partnerships with domestic organizations, such as the Smith Richardson Foundation, the Pacific Council on International Policy, and others have been integral to our research. Moving forward, we will include organizational advocates who can assist at all levels of the public sphere, such as RAND Corporation. We rely on partners to advocate and research effective soft network insulation through speaking engagements, publications, and advocacy.

2. Policy Development

If the National Security Council is unable to conduct a comprehensive process similar to that outlined in Appendix II, we recommend policy development processes that move policy to insulate soft networks in the right direction. We provide two options below:

2.1. *Include Soft Network Policy as Part of the Stabilization Assistance Review (SAR)*: Introduced in 2018, the SAR was a collaborative government effort to improve stabilization efforts and consolidate security accomplishments against non-state actors through efficient bureaucratic structures and decision-making processes rooted in substantiated analysis, cooperation with local and regional partners, and cooperation between various U.S. actors during stabilization efforts. The protection of local national partners falls directly within the purview of the SAR, as the safety of local partners is imperative to local cooperation, and almost all U.S. military and diplomatic actors utilize one form of soft network cooperation or another.

2.2. *Initiate a SAR-like Process Specifically Targeted on Soft Network Protection*: The development of the SAR involved comprehensive analysis and cooperation between various U.S. agencies operating in conflict zones and insecure areas, including the Department of State, U.S. Agency for International Development, and the Department of Defense. Each of these agencies significantly leverages the operational, organizational, and strategic benefits of our soft networks, and, as such, understands the necessity of local national partners. Therefore, should agencies choose not to include soft network protection under the SAR, we recommend initiating a SAR-like policy development process, ideally driven by the NSC. However, a sub-NSC driven process may also yield beneficial results.

Appendix I: Publications and Outreach

This appendix provides further reading and resources for potential policy makers and field operatives concerned about protecting local national partners.

Publications:

1. Miska, S, Warren R., "Protecting Soft Networks: Time to Counter the Enemy's Logical Strategy," *CTX Journal* Vol. 3, No. 4, November, 2013, https://globalecco.org/255
2. Romano S., 2018; *Strategically Protecting Soft Networks*, Pacific Council for International Policy Newsroom, July 2018
3. Romano S., 2018; *Member Launches Project to Protect Conflict Zone Allies*, Pacific Council for International Policy Newsroom, July 2018
4. University of Southern California, Romano S., Asch R., 2019; "Soft Networks," *Public Diplomacy Magazine*, Winter/Spring 2019
5. Miska S., Romano S., 2019; "Too Little, Too Late: Making US Policy to Protect Local Allies More than an Afterthought in COIN/CT Operations" *Small Wars and Insurgencies Journal*, April 2019 https://www.tandfonline.com/doi/full/10.1080/09592318.2018.1552434

Public Speaking Engagements:

SPSN researchers will conduct speaking engagements periodically for the public. Subscribe to our monthly newsletter (https://protectingsoftnetworks.org/) for more information about speaking engagements.

1. Soft Networks Panel at PolicyWest, October 2018: Steve Miska, along with former interpreter Fadi Matti, the Washington Post's Sarah Feinberg, and the Pacific Council's Megan Karsh discussed the issue of protecting soft networks on a panel at the Pacific Council's PolicyWest Conference. Watch here.
2. ISOA Summit Presentation, November 2018: Steve Miska and former Afghanistan and Iraq Ambassador Ryan Crocker discussed the importance of protecting soft networks in stability and peacekeeping operations at a plenary session during the International Stability Operations Association Summit in November 2018.

Resources for Further Research:

1. Non-Military Practices:
    a. InterAction. "The Security of National Staff: Towards Good Practices" *InterAction Report* (2001).
    b. Autesserre, Séverine. "International Peacebuilding and Local Success: Assumptions and Effectiveness." *International Studies Review* (2017).
    c. Fast, Larissa. "Characteristics, Context and Risk: NGO Insecurity in Conflict Zones." www.doi:10.1111/j.1467-7717.2007.01001.x.

2. Cyber-Security:

a. Waters, Gwendolyn. "Social Media and Law Enforcement." *FBI*, FBI, 1 Nov. 2012, https://leb.fbi.gov/articles/featured-articles/social-media-and-law-enforcement
b. "ISIS Targeting Military Members Via Social Media." *Center for Identity*, The University of Texas at Austin, https://identity.utexas.edu/id-perspectives/isis-targeting-military-members-via-social-media.

3. Contracting:
   a. United States. Department of Defense. CENTCOM. CONTRACTOR SUPPORT OF U.S. OPERATIONS IN THE USCENTCOM AREA OF RESPONSIBILITY.October 2018. https://www.acq.osd.mil/log/ps/.CENTCOM_reports.html/5A_October_2018.pdf
   b. 252.225-7040 Contractor Personnel Supporting U.S. Armed Forces Deployed Outside the United States, § DFARS (2015). https://www.acq.osd.mil/log/ps/.ctr_mgt_accountability.html/DFARS_252.225-7040_JAN2015.pdf
4. Foundational Readings:
   a. Packer, George. "Betrayed." *The New Yorker*, The New Yorker, 6 July 2017, www.newyorker.com/magazine/2007/03/26/betrayed-2.
   b. "State-USAID-DoD Stabilization Assistance Review (SAR)." *U.S. Department of State*, U.S. Department of State, 19 June 2018, www.state.gov/r/pa/prs/ps/2018/06/283334.htm.
   c. Jaffe, Greg. "As U.S. Leaves Iraq, Iraqi-Turned-U.S. Soldier Bids Goodbye to Homeland." *The Washington Post*, WP Company, 18 Dec. 2011, www.washingtonpost.com/world/national-security/as-us-leaves-iraq-iraqi-teen-turned-us-soldier-bids-goodbye-to-homeland/2011/12/18/gIQA9Obf2O_story.html?utm_term=.84713683e827.
   d. Miller, T. Christian. "Chart: Iraqi Translators, a Casualty List." ProPublica. December 09, 2009. https://www.propublica.org/article/chart-iraqi-translators-a-casualty-list.
   e. Bruno, Andorra. "Iraqi and Afghan Special Immigrant Visa Programs." *Federation of American Scientists*, Congressional Research Service, 26 Feb. 2016, www.fas.org/sgp/crs/homesec/R43725.pdf.

SPSN Partners & Web Resources

1. Strategically Protecting Soft Networks Website: www.protectingsoftnetworks.org
2. International Refugee Assistance Project Website: www.refugerights.org
3. No One Left Behind Website: http://nooneleft.org/
4. Veterans for American Ideals Website: https://www.vfai.org/
5. The Pacific Council on International Policy: https://www.pacificcouncil.org/
6. The College of International Security Affairs: https://cisa.ndu.edu/

Appendix II: Policy Development Process: National Security Study Directive

A National Security Study Directive (NSSD) process is the gold standard to focus the attention of the interagency on this strategic problem. A NSSD would direct departments and agencies to study the problem over a 6-8 month time period and develop policy solutions. As the project continues, we envision pursuing a policy development plan similar to an NSSD.

Objective: Direct Departments and Agencies to gain understanding of the threat to soft networks (local national partners who enable military and diplomatic missions) and develop policies, doctrine and training to insulate those networks.

Vision: Develop resilience amongst soft networks to withstand adversaries who wage campaigns of intimidation and coercion against America's closest partners abroad, thereby buttressing current operational efforts and cementing gains.

Timeline for NSSD Process (6-8 months)

• 1st Month – call an Interagency Policy Committee to develop the NSSD directive
• Weekly or bi-monthly meetings as the process develops

Department/Agency Roles[29]

National Security Council:

• Shepherd process and track progress

Department of State/ Department of Defense (lead agencies):

• Provide statistics on local national contractor deaths, injuries
• Develop policy options for temporary & permanent relocation across state boundaries
• Develop contracting policy that integrates best practices to insulate soft networks
• Define the scale of local national contractors
• Develop policy, doctrine & training to insulate soft networks
• Develop contracting policy that integrates best practices to insulate soft networks

Directorate of National Intelligence and *Central Intelligence Agency*:

• Provide current and historic threat assessments to soft networks
• Develop 3-5 planning scenarios of likely threats to soft networks to guide department/agency planning during the NSSD process. (i.e. embassy or military interpreter receives death threats via letter from neighbor from militia/insurgent. Threats continue via calls and texts to interpreter cell phone.)

[29] Note: Recommended – stakeholders should participate in refining roles and key tasks

Department of Homeland Security:

• Identify potential domestic threat from SIV program if expanded beyond Iraq/Afghanistan

Department of Justice/Federal Bureau of Investigation:

• Provide identity protection options abroad
• Identify potential domestic threat from SIV program if expanded beyond Iraq/Afghanistan

Office of Management and Budget:

• Provide cost estimates for identity protection and local/temporal relocation options
• Update the cost estimate for the SIV program

Department of Labor:

• Provide data from government contracting firms on interpreters and other local national contractors killed and wounded
• Make recommendations on improvements to government contractor reporting to meet legislative requirements