Enhancing the Effectiveness of the U.S. National Guard's State Partnership Program on Defensive Cyber Capabilities Abroad

By Kevin Heaney

April 2022

Frank Batten School of Leadership and Public Policy

University of Virginia

– Applied Policy Project –

prepared for

Office of the Under Secretary of Defense for Policy, Cyber Policy

U.S. Department *of* Defense

UNIVERSITY *of* VIRGINIA
FRANK BATTEN SCHOOL *of*
LEADERSHIP *and* PUBLIC POLICY

Table of Contents

Cover Images:

Left - Members of the Connecticut National Guard board a C-130 H aircraft enroute to Washington, D.C., January 15, 2021, at Bradley Air National Guard Base, Connecticut. U.S. Air National Guard photo by Master Sgt. Tamara R. Dabney.

Center – Image by Daniil Peshkov

Right - U.S. Army Spc. Quret Ain, a member of Civil Affairs East Africa, in support of Combined Joint Task Force - Horn of Africa (CJTF-HOA), helps a soldier assigned to the Armed Forces of Djibouti (FAD) during a cyber defense engagement at the Sheraton Hotel, Djibouti, Feb. 17, 2021. U.S. Air Force photo by Senior Airman Taylor Davis.

U.S. Department of Defense, University of Virginia, and Frank Batten School of Leadership and Public Policy images and logos are property of those institutions and do not constitute an endorsement of the views expressed within this document.

Acknowledgments

Todd Anderson, my sponsor at OUSDP Cyber Policy, without whom this entire project would have been impossible,

Brenan Richards and Tyler Duke,

Prof. Brad Carson, Prof. Kirsten Gelsdorf, Dr. John Holbein, Dr. Phil Potter, Dr. John Robinson, Dr. Allan Stam, and Prof. Gerry Warburg,

Dr. Nathaniel Allen, CPT Gus Ashton, MAJ Harrison C. Bittenbender, Lt. Col. Walter Dragon, Lt. Col. Janice Hernandez, Campbell Kane, Maria Kingsley, MAJ John Macuga, LTC Art Moore, LTC Kevin J. Murphy, David Radcliffe, COL Brad Rhodes, Dr. Vinothini Roy, Col. Dan Sutch, Elizabeth T. Vish, Stan Wanklyn, and Thomas C. Wingfield,

Alexa Angelo, Savannah Horton, Austin Katstra, Andrew Sharpe, Lizzy Padhi, Haydon Pitchford, and Kaytee Wisley,

Mom, Dad, TJ, Migna, Kerry, Kevin, Kathryn, Koda, and Luke,

Stephen

Thank You
KWPH

Disclaimer & Honor Pledge

The author conducted this study as part of the program of professional education at the Frank Batten School of Leadership and Public Policy, University of Virginia. This paper is submitted in partial fulfillment of the course requirements for the Master of Public Policy degree. The judgments and conclusions are solely those of the author, and are not necessarily endorsed by the Batten School, by the University of Virginia, by the U.S. Department of Defense, or by any other agency.

On my honor as a University of Virginia student, I have neither given nor received unauthorized aid on this assignment.

Acronyms

AM&E – Assessment, Monitoring, and Evaluation

APT – Advanced Persistent Threat

AU – African Union

DoD – U.S. Department of Defense

COCOM – Unified Combatant Command

AFRICOM – U.S. Africa Command

CYBERCOM – U.S. Cyber Command

CRS – Congressional Research Service

DSCA – Defense Security Cooperation Agency

ECOWAS – Economic Community of West African States

GAO – Government Accountability Office

ISG – Institute for Security Governance

ICB – Institutional Capacity Building

IT – Information Technology

LGBTQ+ - Lesbian, Gay, Bisexual, Transgender, Queer, and more community

LOE – Line of Effort

Mil-Mil – Military to military

NDAA – National Defense Authorization Act

NGB – National Guard Bureau

OUSDP – Office of the Under Secretary of Defense for Policy

SPP – State Partnership Program

Executive Summary

The author has been tasked with providing analysis on how to maximize the effectiveness of the U.S. State Partnership Program (SPP) on the topic of defensive cybersecurity training abroad, and this report serves to explore the capabilities required and standards defined to meet that goal. The author also uses Africa as the key example theater for bringing these principles into the real world, due to its unique challenges in cyberspace and technology governance, expected population growth, and importance as a competition space for the U.S. and major competitors.

Existing literature and research suggest the key challenges on this topic are the defensive cybersecurity capacities of various National Guard components and the evaluation systems used to measure the success of security cooperation programs. The options presented here for consideration may bring the necessary skills needed to America's allies and partners and are measurable to understand if training programs under the SPP are successful. Options to be considered include modifications to how the National Guard trains under the SPP in cyber abroad. This report also evaluates the target end state that National Guard units are aiming towards in their partnered relationships. Evaluative criteria include Cost, Feasibility, Foreign Access, and Strategic Interest.

The recommendation is to use the most capable National Guard units to train multiple foreign partners, while augmenting with contracted private sector training teams until more National Guard units are fully capable of conducting this training. Using foreign multilateral organizations is also a way to multiply the effectiveness of the SPP and reach more partner nations. The Office of the Under Secretary of Defense for Policy (OUSDP) and the National Guard Bureau (NGB) should ensure that National Guard units understand their intended goals, collaborate with other capacity building efforts run by the U.S. State Department, and properly implement Assessment, Monitoring, and Evaluation (AM&E) frameworks in Cyber SPP engagements.

Problem Statement

Developing nations with complicated internet landscapes, including in Africa, seek to develop defensive cyber capabilities. One of the ways that the U.S. aims to be the partner of choice for nations is through the U.S.'s State Partnership Program (SPP). However, not every U.S. state's National Guard has robust defensive cyber capabilities ideal for meeting this training need abroad. Additionally, assessment, monitoring, and evaluation (AM&E) of defensive cybersecurity programs are still in development, limiting transparency and accountability, and institutional capacity building is intermittent.

Introduction

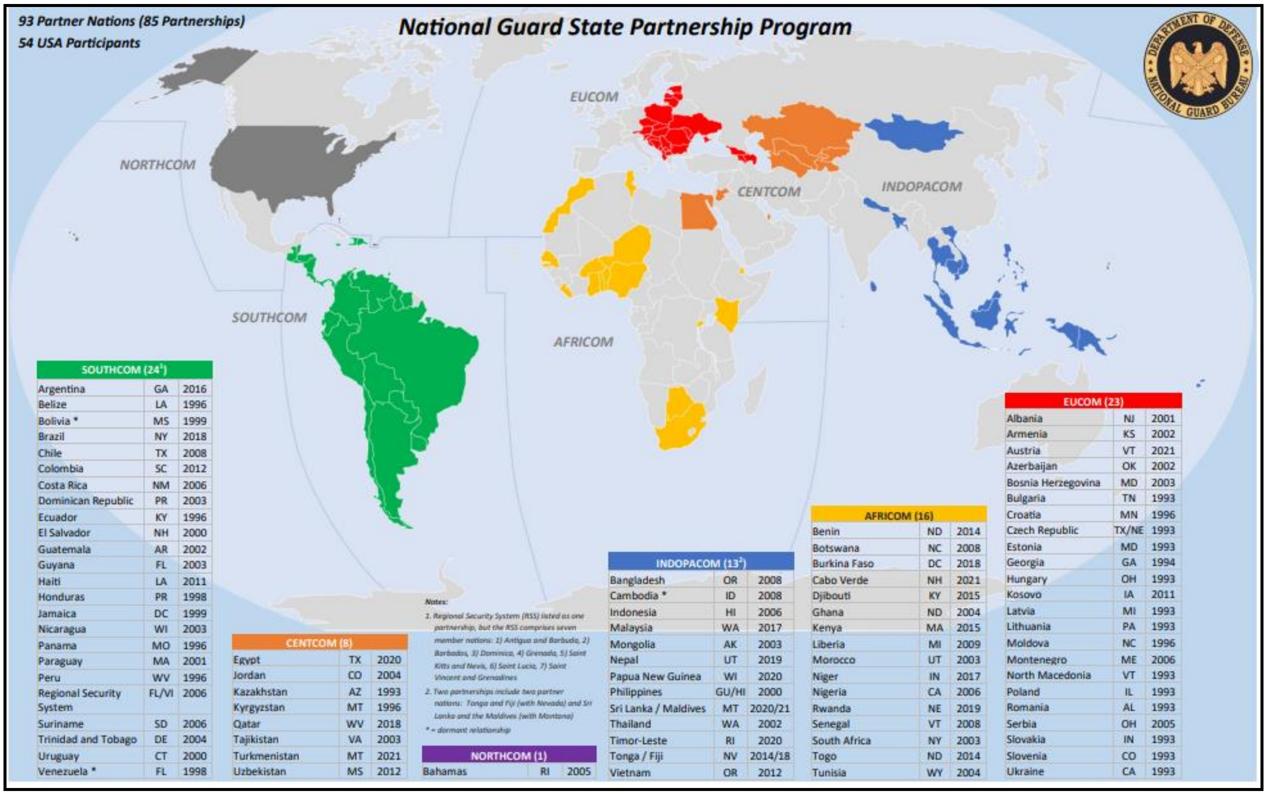
The U.S. Department of Defense (DoD) engages with foreign governments abroad on a military-to-military basis. One of the most successful of these engagement programs is the **State Partnership Program (SPP)**, which partners National Guard units from the 50 American states with foreign militaries in 89 countries. These partnerships are expressly limited to training and exercise purposes. (*State Partnership Program - The National Guard*, 2022) Only

U.S. Cyber Command (CYBERCOM) has authority under Title 10 of the United States Code to "hunt forward[1]" and conduct the cyberspace equivalent of combat engagement with foreign information systems (Borghard & Zabierek, 2021).

In 2019, CYBERCOM's General Paul Nakasone said the following during testimony to the Senate Armed Services Committee: "We are also exploring options with the National Guard State Partnership Program (SPP), which fosters trust with foreign militaries through bilateral engagements with roughly 70 partner nations. While our Command develops our global partnerships in the cyberspace domain, my intent is to work through the geographic combatant commands in growing theater security cooperation efforts." (Nakasone, 2019) Below we can see a comparison of where the SPP is currently engaged with nations abroad, and a map of ongoing (April 2022) botnet[2] attacks. There is significant overlap in the areas of Eastern Europe, Southeast Asia, and southern Africa.

[1] "Hunt forward" operations involve "deploying defensive cyber teams around the world at the invitation of allies and partners to look for adversaries' malicious cyber activity." – U.S. Department of Defense, 2020

[2] "Botnets" are "networks of victim computers surreptitiously infected with malicious software" (U.S. Department of Justice, 2015) that are used for computing power, unbeknownst to their rightful owner.



93 Partner Nations (85 Partnerships)
54 USA Participants

National Guard State Partnership Program

SOUTHCOM (24[1])		
Argentina	GA	2016
Belize	LA	1996
Bolivia *	MS	1999
Brazil	NY	2018
Chile	TX	2008
Colombia	SC	2012
Costa Rica	NM	2006
Dominican Republic	PR	2003
Ecuador	KY	1996
El Salvador	NH	2000
Guatemala	AR	2002
Guyana	FL	2003
Haiti	LA	2011
Honduras	PR	1998
Jamaica	DC	1999
Nicaragua	WI	2003
Panama	MO	1996
Paraguay	MA	2001
Peru	WV	1996
Regional Security System	FL/VI	2006
Suriname	SD	2006
Trinidad and Tobago	DE	2004
Uruguay	CT	2000
Venezuela *	FL	1998

CENTCOM (8)		
Egypt	TX	2020
Jordan	CO	2004
Kazakhstan	AZ	1993
Kyrgyzstan	MT	1996
Qatar	WV	2018
Tajikistan	VA	2003
Turkmenistan	MT	2021
Uzbekistan	MS	2012

Notes:

1. Regional Security System (RSS) listed as one partnership, but the RSS comprises seven member nations: 1) Antigua and Barbuda, 2) Barbados, 3) Dominica, 4) Grenada, 5) Saint Kitts and Nevis, 6) Saint Lucia, 7) Saint Vincent and Grenadines
2. Two partnerships include two partner nations: Tonga and Fiji (with Nevada) and Sri Lanka and the Maldives (with Montana)

* = dormant relationship

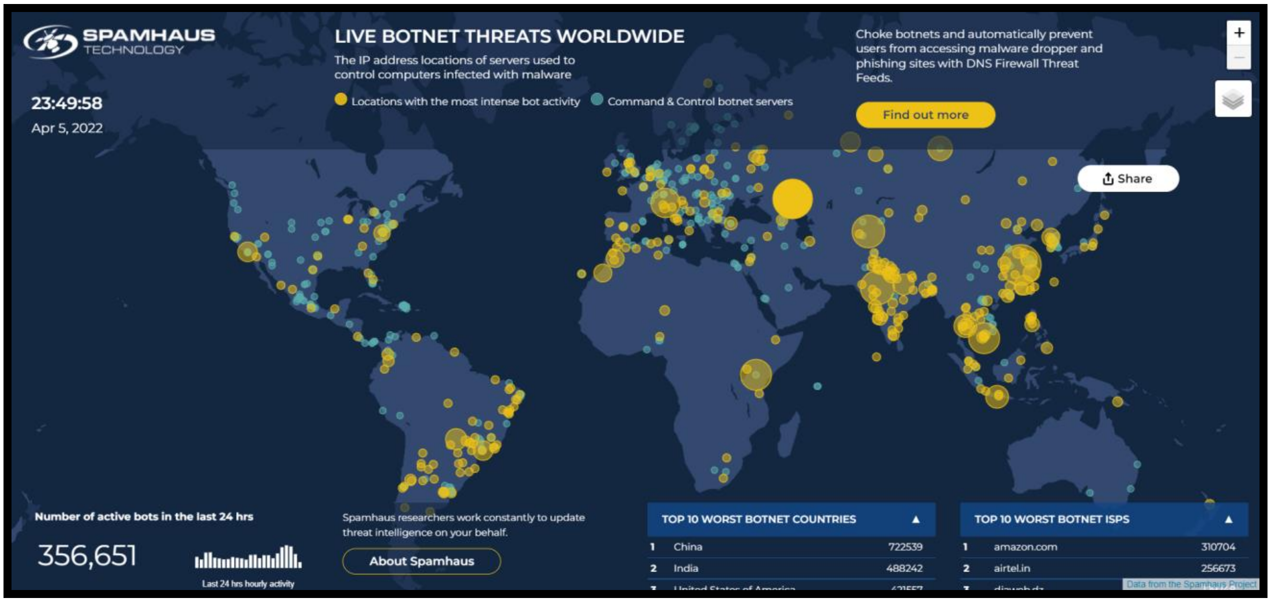
NORTHCOM (1)		
Bahamas	RI	2005

INDOPACOM (13[2])		
Bangladesh	OR	2008
Cambodia *	ID	2008
Indonesia	HI	2006
Malaysia	WA	2017
Mongolia	AK	2003
Nepal	UT	2019
Papua New Guinea	WI	2020
Philippines	GU/HI	2000
Sri Lanka / Maldives	MT	2020/21
Thailand	WA	2002
Timor-Leste	RI	2020
Tonga / Fiji	NV	2014/18
Vietnam	OR	2012

AFRICOM (16)		
Benin	ND	2014
Botswana	NC	2008
Burkina Faso	DC	2018
Cabo Verde	NH	2021
Djibouti	KY	2015
Ghana	ND	2004
Kenya	MA	2015
Liberia	MI	2009
Morocco	UT	2003
Niger	IN	2017
Nigeria	CA	2006
Rwanda	NE	2019
Senegal	VT	2008
South Africa	NY	2003
Togo	ND	2014
Tunisia	WY	2004

EUCOM (23)		
Albania	NJ	2001
Armenia	KS	2002
Austria	VT	2021
Azerbaijan	OK	2002
Bosnia Herzegovina	MD	2003
Bulgaria	TN	1993
Croatia	MN	1996
Czech Republic	TX/NE	1993
Estonia	MD	1993
Georgia	GA	1994
Hungary	OH	1993
Kosovo	IA	2011
Latvia	MI	1993
Lithuania	PA	1993
Moldova	NC	1996
Montenegro	ME	2006
North Macedonia	VT	1993
Poland	IL	1993
Romania	AL	1993
Serbia	OH	2005
Slovakia	IN	1993
Slovenia	CO	1993
Ukraine	CA	1993

Image Source: U.S. National Guard Bureau, Jan 2022



LIVE BOTNET THREATS WORLDWIDE

The IP address locations of servers used to control computers infected with malware

● Locations with the most intense bot activity ● Command & Control botnet servers

Choke botnets and automatically prevent users from accessing malware dropper and phishing sites with DNS Firewall Threat Feeds.

23:49:58
Apr 5, 2022

Number of active bots in the last 24 hrs

356,651

Spamhaus researchers work constantly to update threat intelligence on your behalf.

TOP 10 WORST BOTNET COUNTRIES ▲		
1	China	722539
2	India	488242
3	United States of America	421557

TOP 10 WORST BOTNET ISPS ▲		
1	amazon.com	310704
2	airtel.in	256673
3	djaweb.dz	

Image Source: Spamhaus Technology, April 2022

Client Overview

The Office of the Under Secretary of Defense for Policy (OUSDP) serves to inform the Under Secretary for Policy, the Deputy Secretary, and the Secretary of Defense (SECDEF) on policy matters for the DoD. This insight is particularly vital when policy matters cut across different elements of the DoD, including the uniformed Armed Forces branches, their civilian departments, the reserve components, and DoD agencies including the National Guard Bureau (NGB) and National Security Agency (NSA).

OUSDP will also likely face increased scrutiny over U.S. training and force development efforts abroad following the August 2021 withdrawal of U.S. forces from Afghanistan. Much scrutiny from Congress, media, and the American public is centered around the apparent collapse of the Afghan Armed Forces (Whitlock, 2019). OUSDP is also the DoD office responsible for evaluation of the SPP, with the Defense Security Cooperation Agency (DSCA).

Key Stakeholders

The key stakeholders for this problem vary in jurisdiction and role, primarily on the dividing line of being managed at the state or federal level. That difference impacts funding source, empowering authorities, and the role that the stakeholders can play in either offensive or defensive capabilities.

U.S. National Guard Forces – The 54 National Guard forces of the states, the territories of Puerto Rico, the U.S. Virgin Islands, Guam, and the District of Columbia. The National Guard of each state/territory is largely composed of part-time service members of the U.S. Army and Air Force, who may be activated by their state or territory's Governor (or the President's designee for the District of Columbia, currently the Secretaries of the Army and Air Force) to respond to emergencies under state/territorial authority. National Guard forces may also be "federalized" under Title 10 of the United States Code to serve under the authority of the President and the DoD. Each state's National Guard is led by an Adjutant General, appointed by the Governor.

National Guard Bureau – The National Guard Bureau (NGB) serves as a coordinating entity for the DoD to interface with the 54 National Guard forces. The Chief of the National Guard Bureau is responsible for ensuring readiness of personnel alongside the Departments of the Army and the Air Force. They are also a member of the Joint Chiefs of Staff.

Unified Combatant Commands – Unified combatant commands, more commonly known as combatant commands and COCOMs, are how the DoD organizes and commands forces across the different service branches. The chain of command for U.S. service members starts with the President, through the Secretary of Defense, to the commanders of the COCOMs. COCOMs can either be geographical (such as Africa Command) or functional (such as Cyber Command or Transportation Command).

U.S. Cyber Command – U.S. Cyber Command (CYBERCOM) is the combatant command responsible for the conduct of the military's cyberspace operations, including offensive actions taken against actors abroad. CYBERCOM also partners with foreign nations on a military-to-military basis on cyber and information security matters.

U.S. State Department and Embassy Personnel – Under present security cooperation authorities and regulations, all security cooperation efforts abroad are required to be organized in consultation with the relevant personnel in the partner's U.S. Embassy. Those personnel may include a Military Defense Attaché, a Political-Military Affairs Officer, or an Economic Officer. Additionally, the State Department has just upgraded its Office of the Coordinator to Cyber Issues to a Bureau of Cyberspace and Digital Policy which will be led by an official with Ambassador rank (Schaffer, 2022).

Foreign militaries – Many foreign militaries abroad, particularly from less-industrialized nations, view military-to-military cooperation with the United States as a great source of pride and a way to signal strength to neighbors (McCarthy, 2021).

Background

Cyber Landscape

Internet-connected technology is ubiquitous in our homes, places of work, transportation centers, and commercial hubs. From our home appliances and vehicles to our infrastructure, retail, medical services, to food processing and preparation, there is hardly an element of modern life that is entirely disconnected from the "internet of things" (Burgess, 2018). All of these additional devices and elements dramatically increase the "attack surface" available for exploitation by nefarious actors from money-driven criminals to foreign spies (Brooks, 2021). Global cybercrime is expected to reach $6 trillion in damages in 2021, and estimated to cost $10.5 trillion annually by 2025 (Morgan, 2020). Most countries have not stood up formal cybersecurity response teams or protocols, which likely means that even the alarming amount of recorded events is likely less than the true value of incidents and damages (Allen, 2021).

RAND describes cyber warfare as "the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks." (RAND Corporation, n.d.) Some examples of cyber warfare are more passive, such as social media disinformation or propaganda campaigns. Russia and China have been caught undergoing these types of campaigns in recent years, seeking to increase polarization around US elections and civil unrest around topics such as race. (Scott, 2020)

Africa as the Theater

Cyber conflict arrived in Africa several years ago. Headline-worthy incidents date back to 2012, when the terrorist group Boko Haram allegedly hacked into a Nigerian government database and retrieved information about special forces personnel (Obura, 2017). In response, Nigeria established a Cyber Warfare Command within their army modeled after US CYBERCOM (O'Flaherty, 2018).

Estimates currently suggest that there are about half a billion unique mobile subscribers in sub-Saharan Africa (GSMA Staff, 2021). Northern African countries also report extremely high rates of mobile broadband subscriptions, with rates as high as 96% in Algeria and 77.8% in Tunisia (Saleh, 2021). Mobile money transfer services are common-place in Africa, and usage was expanded during the COVID-19 pandemic as in-person and cash options were restricted (Mureithi, 2021). Online facilitation of smuggling, drugs, and human trafficking have grown rapidly in recent years on the continent (INTERPOL, 2020). One estimate suggests that 90% of African businesses do not have adequate information protection, and that 85% of African banks have suffered cyberattacks (Odonkor, 2020).

Strategic Competition with China and Russia

The costs of the newest and most robust defensive systems may be out of reach for many entities in poorer African nations, including governments, private utilities, and lifeline sectors such as hospitals (Dixon & Balson, 2020). Historical resource exploitation and underdevelopment has left many African nations without the important infrastructure foundation needed for the security schemes that are essential with ubiquitous technological proliferation. This could include secure and stable electrical grids, and other utilities needed for cybersecurity response centers (*Living below the Cyber Poverty Line: Strategic Challenges for Africa*, 2022).

The Chinese government's strategy and success in embedding itself with African countries looking for investments in critically essential infrastructure, such as telecommunications systems, is cause for significant concern. A Center for Strategic & International Studies (CSIS) report found that over half of Chinese telecom company Huawei's deals are in middle to lower income nations, with African countries exceeding all other continents. (Hillman & McCalpin, 2021) Compounding the financial and surveillance risk is the proliferation of phones sold on the continent that have come pre-installed with Chinese-based tracking malware ("Chinese Phones with Built-in Malware Sold in Africa," 2020).

This type of reach is alarming, given the Chinese government's lack of protections for data privacy which could lead to government requests for customer data that companies may be unwilling or unable to deny. In one particularly damning discovery, servers inside the African Union's headquarters were discovered to be transmitting massive amounts of data to Shanghai off business hours without local knowledge (Kadiri & Tilouine, 2018). Other forms of cyber warfare are more direct, including

Key Human Rights Issue: LGBTQ+ Privacy

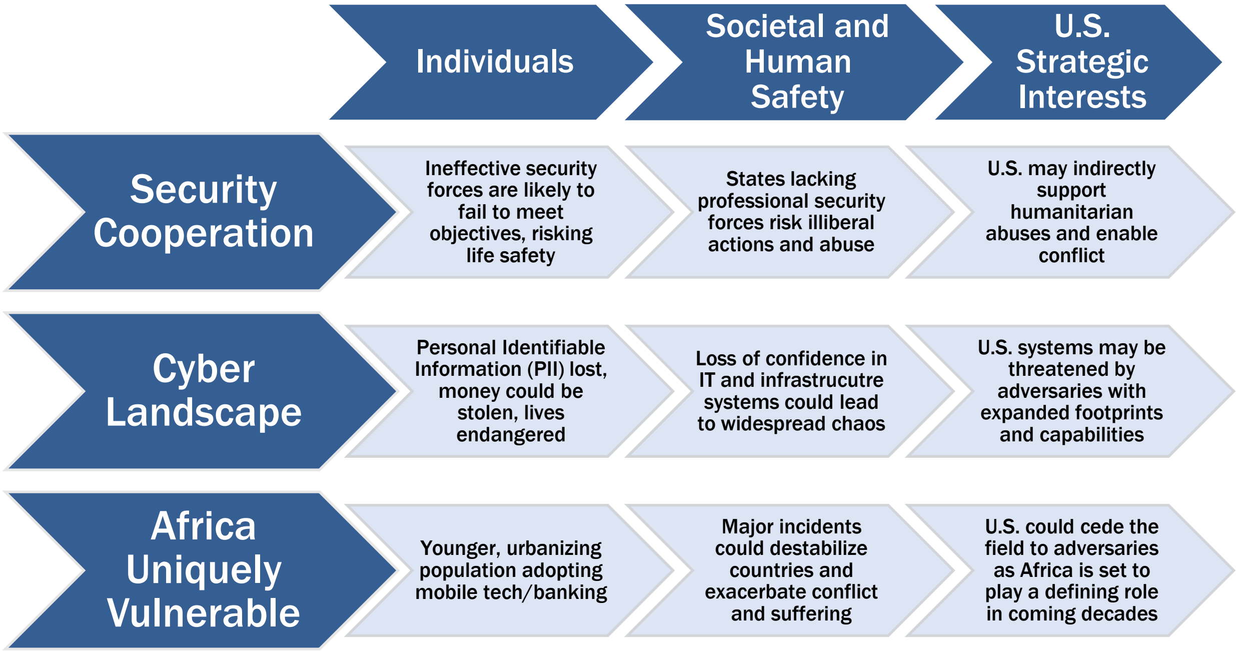
One recent data leak in Morocco "outed" at least 50 men when location data from a primarily gay-serving meeting app was released online. Some of the identified men reported death threats, banishment from their homes and families, and some have considered attempting to flee to other countries in Europe – an option made significantly more difficult by COVID-19 (Alami, 2020). Many LGBTQ+ people find extremely important communities online that can be affirming and even life-saving (Leventry, 2019). However, if these communities are breached and this information published publicly, many individuals would face extreme danger given the continent's continued hostility to LGBTQ+ rights and safety (Hussain, 2020).

state-associated Chinese criminals breaching Microsoft Exchange's email infrastructure and potentially stealing or disrupting system access for millions of the tech giant's customers. (Tucker, 2021)

Meanwhile, Russia has expanded its presence on the African continent and curried favor with rulers by offering the mercenaries of the Wagner Group to several African states. The Wagner Group, acting as a tool of Russian goals but with plausible deniability from Moscow, have been accused of committing human rights abuses and war crimes in Afghanistan, Syria, and Ukraine (Barabanov & Ibrahim, 2021). Stanford University researchers identified suspicious Facebook activity tied to the Wagner Group, with targeted Facebook Pages in Libya, Madagascar, Mozambique, the Central African Republic, the Democratic Republic of the Congo, and Sudan (Grossman et al., 2019). While African countries' perspectives on internet governance are varying, a majority supported a Russian-promoted United Nations resolution which would appear to favor a splintered global internet structure that would allow national governments to wield significant influence inside their own borders – potentially to the detriment of political dissent and human rights groups (Clifford, 2021).

The SPP has already proven to be impactful in response to the 2022 Russian invasion of Ukraine. As California's SPP partner, the Ukrainian military has been training alongside National Guard personnel for decades. Army Major General David S. Baldwin, currently serving as the California Adjutant General, claims that he was more optimistic about Ukrainian capabilities than many media assessments because of his firsthand knowledge gained during SPP engagements. MG Baldwin also served as a connection point between the Ukrainian forces and the DoD as the U.S. developed the list of weapons that we ultimately provided to Ukraine (Garamone, 2022). Additionally, the Indiana National Guard is assisting its Slovakian partners in managing refugee surges from the crisis, as well as shoring up defensive cyber networks across Slovakia (Trares, 2022).

Consequences



	Individuals	Societal and Human Safety	U.S. Strategic Interests
Security Cooperation	Ineffective security forces are likely to fail to meet objectives, risking life safety	States lacking professional security forces risk illiberal actions and abuse	U.S. may indirectly support humanitarian abuses and enable conflict
Cyber Landscape	Personal Identifiable Information (PII) lost, money could be stolen, lives endangered	Loss of confidence in IT and infrastrucutre systems could lead to widespread chaos	U.S. systems may be threatened by adversaries with expanded footprints and capabilities
Africa Uniquely Vulnerable	Younger, urbanizing population adopting mobile tech/banking	Major incidents could destabilize countries and exacerbate conflict and suffering	U.S. could cede the field to adversaries as Africa is set to play a defining role in coming decades

Outlined here is a sense of how the intersecting topics of security cooperation, cybersecurity, and African security affect the various scope levels of individuals, societal and human safety, and U.S. strategic interests.

National Guard Workforce

Carrying out SPP engagements is presently the responsibility of the 54 National Guards across the country and coordinated by the National Guard Bureau. There are presently approximately 60 National Guard cyber units serving 40 states, with some units serving multiple states under agreements (GCN Staff, 2021). Meeting the needs of Federal deployments, state missions, and SPP engagements is likely to place extraordinary strain on all but the largest and most capable National Guard cyber units.

National Guard personnel and leaders report confusion, strain, and a lack of clarity about the long-term success of SPP cyber engagements – even as they personally enjoy working with their foreign counterparts. One unit leader emphasized that their priority was their unit's Federal mission (to support their Service's cybersecurity needs), followed by their state mission, and then the SPP. Several servicemembers report a lack of guidance from NGB about their intended goals for engagement, and some reported trying to develop their own training and development plans for their partners.

During the confirmation hearings for her eventually role as Secretary of the Army, the Honorable Christine Wormuth acknowledged our nation's reliance and potential overuse of National Guard and Reserve forces in recent years. The eventual Secretary promised to review, alongside the National Guard Bureau, the past several years of "virtually nonstop"

National Guard deployments – including response to civil disobedience and worker shortages in various states due to the COVID-19 pandemic (Kheel, 2021).

There is also discontent within National Guard forces about the tempo of recent years. Looking back on recruitment materials advertising "one weekend a month, two weeks every summer" personnel are describing unsustainable strain on their personal and professional lives due to extended and frequent deployments. In recent years, up to approximately one-third of National Guard personnel nationwide have been simultaneously activated (Douglis, 2021).

Many report strain on their civilian professional jobs, and report making less money while on military deployment than their civilian jobs – even to the point of facing risks such as losing their homes or marriages due to the time away (Douglis, 2021). A U.S. Census Bureau report from 2021 found that National Guard and Reserve personnel are more than twice as likely than the average American to report food insecurity, with that number increasing among service members with children (Reilly, 2021).

If the SPP is going to be a successful and worthwhile program for the National Guard, then servicemembers need to understand the full goals and objectives of the program so they know it is a valuable use of their contested time. DoD should also ensure that National Guard forces are being used most effectively when they can be and look for other solutions when a National Guard force may not be the most effective foreign cyber engagement tool.

Cyber Training in the U.S. Military

Presently, the Army and Air Force have training programs to certify their various cyber-related military occupation positions at various time scales. The Army's Cyber Officer Basic Leadership Course is 12 weeks, while the Air Force's Cyber Warfare Operations Officer course is 9.5 weeks. However, the Army's 17C Cyber Operations Specialist (which appears to align most closely with defensive cyber capabilities) requires 45 days of Advanced Individual Training. Similarly, the Air Force's Cyber Surety enlisted position requires 50 days of technical training. While there will be differences in trying to apply U.S. military systems to nascent developing nation's infrastructure, existing training standards should be evaluated and potentially adapted to foreign systems training.

The military service components are continuing to build up cyber forces among their ranks. In 2019, the Army activated the 915th Cyber Warfare Battalion to provide "non-lethal capabilities such as cyber, electronic warfare and information operations." However, when interviewed, the battalion commanders acknowledged that doctrine and training were still under development and that the battalion would essentially be creating new doctrine as it attempts to stand up this unit (Pomerleau, 2021).

A RAND study compared building language skills in the national security workforce to building cyber skills. This comparison is useful when understanding that programming languages are languages of their own. Some of the main findings from the report suggest that the most significant challenge to developing the workforce may be the "talent pipeline," as finding appropriately skilled individuals who can be potentially trained with no relevant experience is a major challenge. Additionally, the report emphasizes that shared "definitions, training standards, and metrics" are key for success (Li & Daugherty, 2015).

Evaluating Security Cooperation

The SPP is one type of security cooperation program, unique in its usage of state National Guard forces to engage with foreign militaries in comparison to other security cooperation programs which rely on Active Duty forces. The evaluation of U.S. security cooperation programs is a limited but growing field of literature and proposed methods.

Evaluation of the SPP is not only important for internal validation of efforts and dollars spent, but also to determine goals and objectives are being met and risk are effectively being reduced. Understanding the potential risks also underscores the importance of evaluating which countries are being best impacted by U.S. partnership. Whether the decision is to put more resources into the areas that need greatest improvement or to cut losses where performance is unacceptable, those decisions can only be made after a standardized evaluation process occurs.

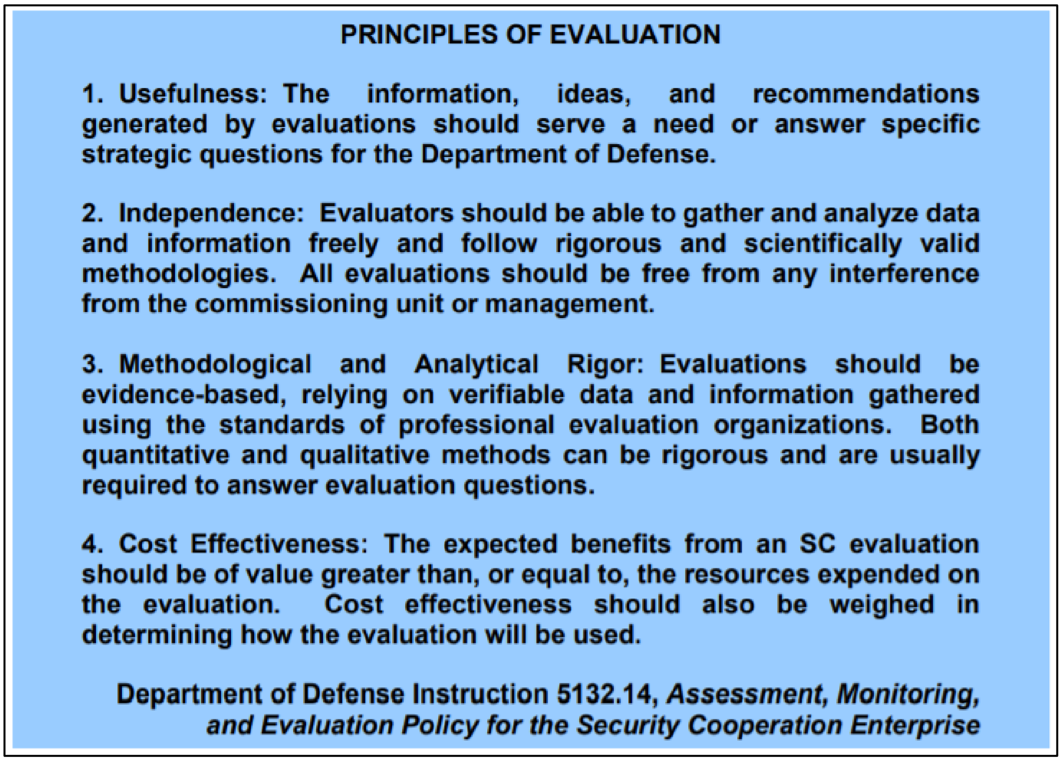
Researchers also argue that U.S. officials should be concerned about whether "purely defensive" capabilities are likely to remain that way or not. Dr. Nathaniel Allen of the National Defense University argues that some African governments' history of abuse of the internet is reason for the U.S. to ensure that our efforts do not "strengthen the capacity of authoritarian regimes or illiberal forces within a particular government" (N. Allen, personal communication, November 2, 2021).

Over the course of the War in Afghanistan, U.S. military and defense officials repeatedly reported to Congress and the public that progress was being made with the strength and capabilities of the Afghan National Army and the Afghan National Police (Gibbons-Neff, 2019). Ultimately those forces were unable to prevent the routing of the U.S.-backed Ghani government in Kabul and the Taliban takeover of the country after twenty years and an estimated $88 billion spent on the development of those security forces (Bender & McLeary, 2021). A robust and publicly available evaluation system may have revealed some of the greater flaws in the attempted development of a legitimate, accountable Afghan Armed Forces.

Existing Law and Policy

In the National Defense Authorization Act (NDAA) for FY2017, Congress enacted reforms to security cooperation programs by requiring assessment, monitoring, and evaluation (AM&E) schemes. DoD Instruction 5132.14 "Assessment, Monitoring, and Evaluation Policy for the Security Cooperation Enterprise" outlines OUSDP's role in AM&E for security cooperation.

The Office is tasked with "Storing and disseminating, across DoD Components, lessons learned derived from evaluations, including briefings of evaluation findings, best practices, and recommendations to relevant DoD Components, before program planning for the following fiscal year." The Instruction prioritizes Usefulness, Independence, Methodological and Analytical Rigor, and Cost Effectiveness in evaluation of security cooperation programs. (U.S. Department of Defense, 2017)



PRINCIPLES OF EVALUATION

1. Usefulness: The information, ideas, and recommendations generated by evaluations should serve a need or answer specific strategic questions for the Department of Defense.

2. Independence: Evaluators should be able to gather and analyze data and information freely and follow rigorous and scientifically valid methodologies. All evaluations should be free from any interference from the commissioning unit or management.

3. Methodological and Analytical Rigor: Evaluations should be evidence-based, relying on verifiable data and information gathered using the standards of professional evaluation organizations. Both quantitative and qualitative methods can be rigorous and are usually required to answer evaluation questions.

4. Cost Effectiveness: The expected benefits from an SC evaluation should be of value greater than, or equal to, the resources expended on the evaluation. Cost effectiveness should also be weighed in determining how the evaluation will be used.

Department of Defense Instruction 5132.14, *Assessment, Monitoring, and Evaluation Policy for the Security Cooperation Enterprise*

Image Source: The Joint Staff, 2017

Instruction 5312.14 also states that, “Unclassified summaries of the evaluation of DoD security cooperation activities will be made publicly available, unless it is determined that disclosure of the summary information could be expected to cause foreseeable harm to the United States or a partner nation.” These unclassified summaries are not currently available online.[3]

Joint Publication 3-20: Security Cooperation was released by The Joint Staff in 2017 following the release of DoD Instruction 5132.14. This guidance says that evaluations should take place at different command levels by officers with different objectives in mind. Unit commanders operating at the tactical level should evaluate programs based on the successful completion of individual tasks. Higher level commanders should be evaluating whether units are “creating the necessary effects and achieving objectives.” The guidance calls for the use of SMART (specific, measurable, actionable, results-oriented, time-bound) objectives.

[3] As of April 2022

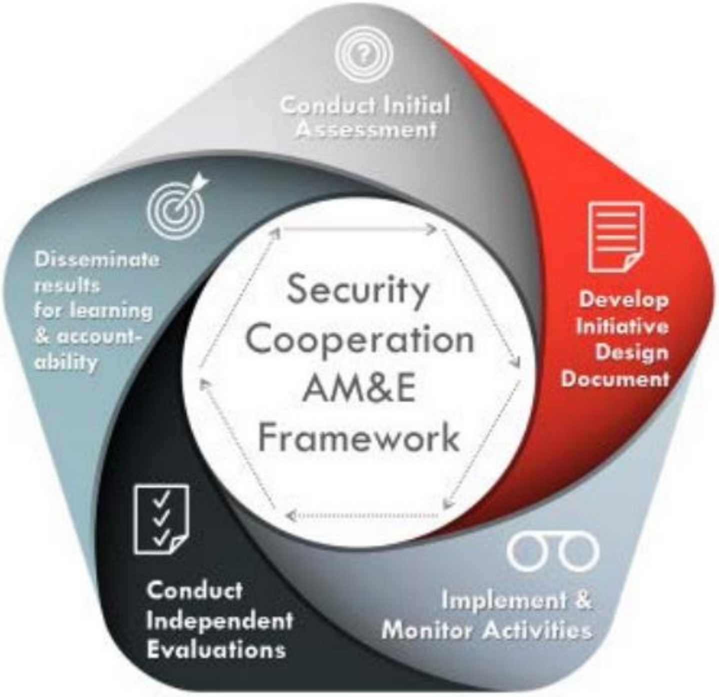

Conduct Initial Assessment
Develop Initiative Design Document
Implement & Monitor Activities
Conduct Independent Evaluations
Disseminate results for learning & accountability
Security Cooperation AM&E Framework

Image Source: DoD Instruction 5132.14

Methods of Evaluation

Some proposed methods of evaluation are almost entirely focused on the characteristics of the partnered nation rather than technical outcomes. Published in 2018, The RAND Corporation conducted a significant review of Army security cooperation programs. RAND conducted analysis based on data from the Global-Theater Security Cooperation Management Information System (G-TSCMIS) maintained by the DSCA. This system stores security cooperation data for all service branches across the DoD (O'Mahony et al., 2018). The authors take note of likely missing data in the system, as well as the notion that different cooperation events were entered into the system similarly, but that different events (such as a site visit compared to a major multinational exercise) should not be compared at the same level.

RAND broke country characteristics into five groups: strategic considerations (including GDP and support for US votes at the United Nations), political considerations, (including respect for human rights, state fragility, and number of recent coups), absorptive capacity considerations (including high school graduates of military service age, share of GDP spent on military, and military technical capability and professionalism), cultural considerations (measured by percentage of the population that speaks English) and financial considerations (such as average dollar amounts of financial assistance).

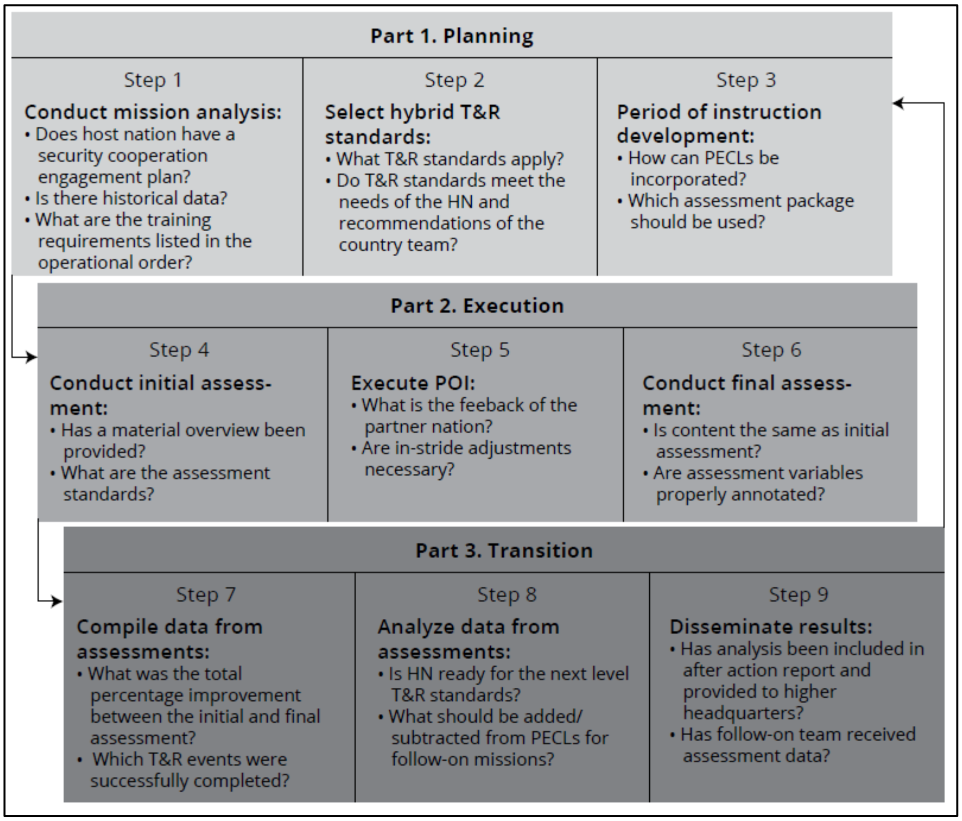
The authors use "percentage of the population that speaks English" as a stand-in for how well foreign military personnel can communication with U.S. servicemembers, their likely ties to common international institutions, and the foreign personnel's "ability to be influenced by the same global media." They do not elaborate on the relationship between

English-speaking media consumption and the benefits of military-to-military engagement. However, it is worth noting that China has been investing in Chinese language schools in nations where they make infrastructure investments under the Belt and Road Initiative (Zhou, 2019).

The study finds that AFRICOM had the lowest security cooperation participation rate among the Geographical Combatant Commands (GCCs) with partner nations attending an average of 7 out of 1,000 total partnership activities. AFRICOM also reports that it is most likely to have partnership events focused on developing “professionalization” by the system’s accounting. This is likely due to the governance challenges in militaries across the continent, including corruption and potential for abuse (Griffiths, 2016).

Pre- and Post-Tests

Other proposed evaluation methods focused on measures conventionally used in teaching and training, such as a pre- and post-test. A review of U.S. Marine Corps documentation including policies and doctrine found that there was a lack of identifiable quantitative metrics that had been identified as suitable for evaluating security cooperation programs. The existing guidelines were based off training and readiness standards. However, this relies on the accuracy of those standards and are constructed differently than combat performance measures (Van Eerden, 2020). Van Eerden recommends adopting a model he developed entitled the “Hybrid Training and Readiness Assessment Methodology.” The model can be found below.



Part 1. Planning

Step 1

Conduct mission analysis:
- Does host nation have a security cooperation engagement plan?
- Is there historical data?
- What are the training requirements listed in the operational order?

Step 2

Select hybrid T&R standards:
- What T&R standards apply?
- Do T&R standards meet the needs of the HN and recommendations of the country team?

Step 3

Period of instruction development:
- How can PECLs be incorporated?
- Which assessment package should be used?

Part 2. Execution

Step 4

Conduct initial assessment:
- Has a material overview been provided?
- What are the assessment standards?

Step 5

Execute POI:
- What is the feeback of the partner nation?
- Are in-stride adjustments necessary?

Step 6

Conduct final assessment:
- Is content the same as initial assessment?
- Are assessment variables properly annotated?

Part 3. Transition

Step 7

Compile data from assessments:
- What was the total percentage improvement between the initial and final assessment?
- Which T&R events were successfully completed?

Step 8

Analyze data from assessments:
- Is HN ready for the next level T&R standards?
- What should be added/subtracted from PECLs for follow-on missions?

Step 9

Disseminate results:
- Has analysis been included in after action report and provided to higher headquarters?
- Has follow-on team received assessment data?

Image Source: Van Eerden, 2020

Evaluating Defensive Cyber Capabilities

Evaluation of defensive cyber capabilities specifically is a developing field. Some existing models primarily use simulations to evaluate defensive capabilities. These models are built around potential cyberattacks and then evaluate the response and recovery capabilities of actors, primarily commercial operators (Legato & Mazza, 2017).

Some scholarship cites the specific challenges between comparing other forms of intelligence activities to cybersecurity activities (Work, 2020). The U.S. Military Academy at West Point has constructed an Information Warfare Analysis and Research (IWAR) Laboratory. The purpose of this laboratory is to translate the familiar concept of a military "firing range" where live ammunition can be used safely under rigorous oversight, to the cyber domain. The IWAR is built to mirror what a military base's information networks may appear like, so that cadets can attempt to build network security mechanisms and defend from real tools that are commonly used by malicious actors outside a classroom environment (Schepens et al., 2002). This also allows operators to be challenged without risking a real functional network that may be vulnerable to espionage or breach.

Exercises are another way to evaluate defensive cyber capabilities. Exercise Cyber Shield is a recurring exercise focused on evaluating defensive cybersecurity efforts across National Guard units. The two-week exercises include portions where National Guard personnel are tested by "train adversaries" (Smith, 2018). In 2021, the Minnesota and Iowa National Guards joined the Kosovo Security Forces and Croatian Armed Forces to conduct Exercise Adriatic Thunder. The exercise involved a "red team" on offense and a "blue team" on defense (Nemec, 2021).

Specific to SPP

In 2011, the Congressional Research Service (CRS) issued "The National Guard State Partnership Program: Background, Issues, and Options for Congress." The CRS attempted to analyze the specific complaint that SPP programs were not always aligned with combatant command (COCOM) leadership and U.S. ambassadors' strategy and objectives for a particular region/country. However, they stated "It is difficult to assess the validity of this criticism with the limited data available." Lack of data and evaluative criteria is a consistent problem when attempting to evaluate the SPP (Kapp & Serafino, 2011).

The Government Accountability Office (GAO) released a 2012 report entitled, "Building Partner Capacity: Key Practices to Effectively Manage Department of Defense Efforts to Promote Security Cooperation." They found that there were multiple systems used to track SPP activities, but that these "are not interoperable and users apply varying methods and definitions to guide data inputs." The GAO found that the National Guard Bureau (NGB) and differing regional COCOMs both used different databases to track SPP activities, as well as different terminology to define various types of foreign engagements (St. Laurent, 2013).

The GAO also found that host nation financial sustainment was a key metric missing from security cooperation evaluations. While conducting interviews, they found that only 1 of the 15 Security Assistance Officers interviewed indicated that the partner nation could sustain their training programs on its own. If programs are not sustainable without direct U.S. financial investment, that would likely be a useful metric for determining where best to allocate resources. This review also specifically calls out the SPP and AFRICOM for not having sufficient frameworks or long-term objectives to evaluate programs. The GAO states that without a clear system of metrics or some way to analyze effectiveness, the program is largely unaccountable.

The SPP has recently drawn the attention of federal lawmakers. In September 2020, Congressman Steve Womack and Congressman Dutch Ruppersberger requested an updated review of the SPP from the GAO, following the 2012 review cited above. Their questions revolve around SPP "goals, objectives, metrics, and milestones" and "sufficient mechanisms in place to accurately and consistently assess individual SPP programs according to those goals, objectives, metrics, and milestones?" (*Womack, Ruppersberger Request GAO Review of National Guard State Partnership Program*, 2020)

Evaluating the success of Cyber SPP engagements is a complicated task, requiring analysis of emerging technologies and skills to be maintained and conducted by many different entities across jurisdictions and authorities. However, strengthening AM&E in the future will be key to ensuring confidence in Cyber SPP and knowing that the program is a worthwhile investment of time and funds.

Evaluative Criteria

As OSD Policy evaluates options for strengthening the effectiveness of Cyber SPP engagements, several criteria will be key to evaluating policy options. These criteria are essential factors in ensuring the success of the program.

Cost

A key criterion for evaluating policy choices is cost. Taxpayer dollars should be used as effectively as possible. One of the main costs to be considered in training programs is personnel, including the National Guard or other personnel deployed by the DoD to conduct the training. Reporting around recent National Guard deployments suggested costs of approximately $530 per service member per day in 2020 (Ali & Brice, 2020). Adjusting DoD payroll records analyzed by McKinsey and Company and ultimately reported in the Washington Post, the average U.S. Army contractor would cost the DoD $794.56 per working day in 2020 dollars, or almost 150% of the service member cost. We can use examples like this to predict potential comparative costs of using National Guard personnel versus contracted personnel.

One category of SPP costs is based around information technology (IT) equipment. DoD purchases IT equipment for partner nations, in some circumstances through the relevant GEOCOCOM. A challenge around IT equipment costs is that they will frequently need to be updated or patched, and some partner nations are unable to support or continue maintenance on equipment after their commercial warranty expires.

New York City Economic Development Corporation is seeking to build the city's cybersecurity talent base by launching "Cyber NYC", which is estimated to cost about $30 million. The plan calls for a new cybersecurity talent and development center, a "cyber boot camp" through local universities, and a venture capital endeavor (Crichton & Tabatabai, 2018). This is just one potential example of the costs associated with building up the cybersecurity capabilities of a major city that is comparable to a small country.

An important trade-off and opportunity cost to consider when evaluating the SPP is that engagements abroad take units away from either their Federal deployment or activation missions, or their state missions – ranging from emergencies like extreme weather to election security work for state cyber units.

Feasibility

An important question worth evaluating when examining new training methods is "Is this feasible?" Interviews with National Guard personnel reveal the many challenges that some partner nations face when it comes to any kind of basic cybersecurity or internet governance. While there are promising signs of serious interest in cybersecurity from multilateral African organizations including the ECOWAS-EU West African Response on Cybersecurity and Fight Against Cybercrime and African Union Mechanism for Police Cooperation's Cybercrime Strategy 2020-2024, experts suggest that national-level cybersecurity efforts are falling behind with only 17 of 54 African countries developing a national cybersecurity strategy (Ajijola & Allen, 2022).

National Guard personnel sometimes report that foreign military partners purchase cyber tools that they do not know how to operate, hoping that a new tool may be a “silver bullet” that protects their networks. Given the potential authority issues that may constrain National Guard personnel from engaging in “offensive” cybersecurity work, SPP engagements may be prohibited from training involving such tools. Much media speculation around the fall of Afghanistan focused on the dependency of the Afghan National Forces upon U.S.-paid contractors for repairs and maintenance (Gibbons-Neff et al., 2021).

DoD Instruction 5132.14 outlines “The feasibility of achieving successful outcomes based on a partner’s political willingness to pursue the desired outcome; its absorptive capacity, including the extent to which a partner can support, employ, and sustain assistance independently; its political stability; and its respect for rule of law and human rights.” (U.S. Department of Defense, 2017)

Foreign Access

The State Partnership Program is required by law to “support the security cooperation objectives of the United States” (*State Partnership Program - The National Guard*, 2022). One of those stated objectives is to "Provide Access” for U.S. military operations around the globe (The Joint Staff, 2017). Therefore, when evaluating policy options for the enhancement of the SPP, it must be considered whether policy choices will promote access to foreign nations for U.S. military operations now and in the future.

The most frequently cited example of the best “Cyber SPP” relationship is Maryland-Estonia. This partnership began in 1993 and Estonia was still in an extremely nascent stage with its cyber capabilities and governance. Presently, U.S. and Estonian cyber personnel are working in full integration to repel Advanced Persistent Threat (APT) actors including Russia. Because of their relationship and the amount of trust developed, Maryland National Guard has information sharing agreements no other DoD or USG elements possess with Estonia. This is one example where a greatly imbalanced relationship that started with SPP training has resulted in an avenue for full access for the U.S. military to integrate with a foreign partner in responding to rival aggression in cyberspace (McLaughlin, 2019).

Strategic Interest

Does this advance larger U.S. national security goals, particularly against Russia and China?

President Biden’s Interim National Security Strategic Guidance (March 2021): “We will renew our commitment to international engagement on cyber issues, working alongside our allies and partners to uphold existing and shape new global norms in cyberspace.” (The White House, 2021)

National Cyber Strategy, September 2018: “Through cyber capacity building initiatives, the United States builds strategic partnerships that promote cybersecurity best practices through a common vision of an open, interoperable, reliable, and secure Internet that encourages investment and opens new economic markets. In addition, capacity building allows for additional opportunities to share cyber threat information, enabling the United States Government and our partners to better defend domestic critical infrastructure and global supply chains, as well as focus whole-of government cyber engagements. Our leadership in building partner cybersecurity capacity is critical to maintaining American influence against global competitors." (The White House, 2018)

Summary of the National Defense Strategy, October 2018: "In consultation with Congress and the Department of State, the Department of Defense will prioritize requests for U.S. military equipment sales, accelerating foreign partner modernization and ability to integrate with U.S. forces. We will train to high-end combat missions in our alliance, bilateral, and multinational exercises." (U.S. Department of Defense, 2018b)

Summary of the Defense Cyber Strategy, September 2018: "Third, the Department will work with U.S. allies and partners to strengthen cyber capacity, expand combined cyberspace operations, and increase bi-directional information sharing in order to advance our mutual interests." "The Department will work to strengthen the capacity of these allies and partners and increase DoD's ability to leverage its partners' unique skills, resources, capabilities, and perspectives. Information-sharing relationships with allies and partners will increase the effectiveness of combined cyberspace operations and enhance our collective cybersecurity posture." "The Department will work alongside its interagency and international partners to promote international commitments regarding behavior in cyberspace as well as to develop and implement cyber confidence building measures (CBM)." (U.S. Department of Defense, 2018a)

Engagement with our partners must be consistent with the goals outlined in each of these strategies, which clearly seek to expand our cooperation and effectiveness with partners in cyberspace.

Policy Options

1. Status Quo

The current status quo is that cyber engagement through the SPP is sporadic and comparatively ill-defined. National Guard personnel admit that only a fraction of state units can conduct this training abroad. Additionally, some unit leaders report uncertainty about the path forward for severely underdeveloped nations or how to proceed with low governance and technical capabilities.

Cost – While not every state is conducting this training abroad, unclear goals and evaluation for Guard personnel may lead to wasted time and effort. Medium Cost.

Feasibility – This is the current status quo, where Guard units are attempting to move forward with limited guidance. However, personnel report challenges on how to develop training with partnered forces. Low Feasibility.

Foreign Access – While many partnered nations appear eager to conduct this training with the U.S., challenges in long-term skill development are not likely to build enduring relationships. Low Foreign Access.

Strategic Interest – This option does not take full advantage of U.S. capabilities and leaves openings for adversary nations to fill the gaps when foreign nations seek training partners of choice. This is particularly true of Chinese engagement in Africa. Low Strategic Interest.

2. Use most capable National Guard cyber units to train multiple partner nations

As the SPP presently stands, U.S. states and partnered nations are matched based on any wide range of reasons which may be based on factors other than military compatibility. A former senior DoD official says that "the SPP provides less subject matter expertise than it does continuity of relationship." Pairings may not be based on which states have maximum capabilities in a partnered country's greatest needs. One option is to re-align Cyber SPP pairings so that countries can be partnered with the National Guard units that excel in the focus area where they may have the greatest need, regardless of their initially designated SPP partner nation.

Cost – This option would use existing National Guard units but may require the most capable units to conduct more training missions abroad since they are in higher demand. Costs could be offset by savings from not sending other units abroad. Medium Cost.

Feasibility – This is a moderately feasible option, as it would leverage units that currently excel at conducting cyber training under the SPP and maximize their talents. However, these units would face significant time commitments and would need to be backfilled at times. Medium Feasibility.

Foreign Access – This option would promote successful training with partnered nations, making the U.S. the security cooperation partner of choice. High Foreign Access.

Strategic Interest – Successful training relationships with partners abroad would promote U.S. success and foreign nation alignment against rival nations. High Strategic Interest.

3. Fusion units built out of the states with the most capable Guard cyber units until all states have fully robust units

This option would form new SPP cyber training units composed of personnel from multiple states. These new teams would be based around skillsets or specific defensive cyber topics and would engage with partnered nations abroad as needed based on the topic.

Cost – This option would use current National Guard personnel but would not mobilize entire cyber units at the same time. This would minimize disruption back home in the state. However, coordination of this system would require significantly more central management. Medium Cost.

Feasibility – This option would require considerable coordination from a centrally located administrator, who would be required to compose the fusion teams based on knowledge of all the individual skillsets of cyber soldiers and airmen across the entirety of all 54 National Guards. Low Feasibility.

Foreign Access – Partner nations will benefit from successful training conducted by U.S. military service members. However, these personnel are more likely to rotate than other policy options and interpersonal relationships would not likely be as strong. Medium Foreign Access.

Strategic Interest - Successful training relationships with partners abroad would promote U.S. success and foreign nation alignment against rival nations. High Strategic Interest.

4. Contract Out

While the current SPP relies exclusively on National Guard personnel, it may be more prudent for the DoD to contract out certain defensive cyber training to appropriate private sector partners based in the U.S. Many familiar defense contractor organizations already conduct cybersecurity training for domestic U.S. customers and could be used to train defensive cybersecurity teams abroad. Some of these companies may also be more familiar with conducting training overseas if they have previously worked with multinational corporations.

Cost – This would likely be a high-cost contract to one or more private sector companies. Contracted work has the potential for cost over-runs and high overhead costs. High Cost.

Feasibility – This option would outsource most of the work to private companies, which may have more resources to be able to be exclusively focused on training development unlike National Guard forces which have multitudes of responsibility. High Feasibility.

Foreign Access – Foreign partners may have less loyalty to U.S. – based companies than they would to U.S. military personnel. Additional efforts would have to be made to reinforce that the U.S. is the nation conducting this training, rather than merely the company. Medium Foreign Access.

Strategic Interest – Partnered nation skills would be strengthened (and therefore less exploitable by adversaries), but the U.S. may not be fully seen as the "partner of choice" by foreign military personnel who would be interacting with civilian contractors instead of uniformed U.S. soldiers and airmen. However, contracted personnel may also be seen as less colonizing or confrontational by nations which have had strained relationships with the West and former colonial powers. High Strategic Interest.

Options and Criteria Matrix

	Criteria			
Policy Option	Cost	Feasibility	Foreign Access	Strategic Interest
Status Quo	Medium	Low	Low	Low
Use Most Capable Units for Multiple Partners	Medium	Medium	High	High
Fusion Units from Multiple States	Medium	Low	Medium	High
Contract Out	High	High	Medium	High

Recommendation

Based on the evaluative criteria, the best course of action is for the DoD to capitalize on the skills of the **Most Capable Units for Multiple Partners** while defensive cybersecurity skills and personnel proliferate throughout the National Guard. These units should be augmented with **Contractors** to better advance U.S. goals abroad in the short-term while domestic capabilities are enhanced.

Existing relationships may not be the best pairings for defensive cybersecurity development between domestic states and foreign military partners. Advanced state units should be leveraged while others get up to speed. In the meantime, DoD should leverage private sector resources to fill in the gaps in the short-term. Contracted training teams can be sent to foreign partner nations with specific, identified skills gaps and training needs in defensive cybersecurity.

While using "Fusion Units" made from personnel from different states may be appealing to try and get the most out of existing personnel, the logistical requirements involved, and frequent unit rotation, would likely negate any potential cost benefits.

Implementation

Executive buy-in will be an important part of implementation for these changes, coming from OSD Policy. Implementing these changes will require making significant reforms within NGB, and how the states' Army and Air National Guards manage and deploy their forces abroad. State officials to potentially include Adjutants General and Governors would need to be briefed and persuaded.

Trade-Offs and Obstacles

One significant trade-off for this recommendation would be Cost. The most capable cyber units throughout the National Guard would be called up more frequently for SPP engagement abroad. Backfilling may be required to ensure that state and other federal missions are still being consistently met by required National Guard units, at a time when cybersecurity skills are in incredible demand across the nation (Marks, 2021).

Additionally, the idea of not using National Guard personnel may be unpopular both within the states and with partner nations. While both parties generally may enjoy the relationships developed through the SPP, the benefits of greater immediate access to training for partner nations and relief for Guard personnel already heavily used for both state and federal missions may become apparent over time. The State Department uses private sector partners including MITRE, Carnegie Mellon University's CERT Division, Software Engineering Institute, George C. Marshall Foundation, and CSIS in its capacity building efforts abroad.

One potential fix for equipment challenges may be to use open-source software. There are many pros and cons to using open-source software, but it may be a viable option for developing nations who face issues maintaining commercial proprietary software or equipment past their warranty lifetimes. Open-source software may be constantly worked on by potentially thousands of developers identifying bugs and other vulnerabilities. Of course, this does raise potential security concerns, as such software is potentially vulnerable to a supply chain-style infiltration attack ("Pros & Cons of Open Source in Business," 2018).

Best Practices from National Guard Unit Leaders

National Guard cyber leaders in multiple states stressed the importance of comprehensive lines of effort (LOEs) coming "down" from the COCOMS to include the relevant GCC and CYBERCOM, National Guard personnel including SPP managers and cyber unit leadership, and the Embassy personnel in the partner nation. This type of coordination spanning multiple DoD and USG elements was reported as critical for effective communication and comprehensive strategy around building foreign nation capabilities.

One National Guard cyber unit leader from a proactive SPP state described practices that promoted success:

- Internal training for new, mid-tier, and advanced personnel so that training programs have already been worked and fine-tuned before they are attempted with foreign partners.
- Identified equipment, and some designated for partner-work only (for security purposes). A separate National Guard cyber unit leader reiterated this challenge, pointing out that certain technologies can't be shared with foreign military actors – even partner nations.
- Clear expectations from the partner nation including expected amount of training time, classroom vs keyboard learning, level of experience, and equipment status/limitations.

National Guard unit leaders must know the private sector skills of their personnel (particularly those working in IT and cybersecurity jobs outside of their military role). By keeping track of professional certifications and other outside development, leaders can ensure that personnel are being used most effectively.

Best practice recommendation from National Guard leaders promotes in-depth coordination between GCCs and in-country partners such as U.S. Embassy personnel. The Instruction also states, "When possible, DoD should align its AM&E efforts with those of host nation counterparts, other donors, and implementing partners. This should lessen the overall data collection burden and help promote security cooperation effectiveness." Further collaboration with the State Department and Embassy personnel will be further discussed below.

Training Development, and AM&E

The DSCA's Institute for Security Governance (ISG) has resources around Cyberspace Capacity Building and Cyber Defense Workforce Training. This includes cybersecurity maturity models, descriptions of relevant job and duty roles, and the frameworks for developing cybersecurity talent. These resources should be heavily relied upon, as they can be used to delineate different essential functions and job categories that need to be developed in partner nations. They can also guide which National Guard personnel or contractors need to be sent abroad to assist partner development in defensive cyber capabilities. Membership in the Forum of Incident Response and Security Teams (FIRST) (a global organization of computer security teams) is a useful benchmark that the State Department uses for its capacity building efforts abroad. Adopting of similar international standards could be a useful benchmark for the DoD to adopt as it seeks to evaluate success in building defensive cyber capabilities abroad through the SPP.

At this point in time, the National Guard Bureau has not laid out standardized policies or practices for National Guard units to conduct AM&E during SPP engagements abroad in cyberspace. Presently, evaluation relying on pre- and post-test assessments is challenging. Baseline capability levels are different between countries, and therefore unreliable. Data is hard to obtain from partner nations, and evaluations end up relying on qualitative data. DoD intends to move to a "Learning Agenda" model that identifies essential knowledge gaps, and then builds learning activities to fill gaps. Questions that will be stressed include, "Are we building capabilities?" and "Which parts did we contribute to in the partner nation?" (M. Kingsley, personal communication, January 28, 2022).

Multilateral Engagement

Regional Cooperation should be promoted where foreign nations can be elevated to similar levels of their most successful neighbors or like countries that have exceled in developing defensive cybersecurity practices and capabilities. The DoD and other U.S. agencies (to include the State Department) should work directly with multilateral institutions such as the African Union and ECOWAS in developing and promoting common defensive cybersecurity standards and practices throughout their areas of membership. The AU and ECOWAS have subgroups focused on IT and cyber issues, which are potential venues for engagement on defensive cybersecurity capacity building.

Joint Publication 3-12, Cyberspace Operations, provides guidance for integration on cyberspace operations across the entire DoD enterprise. In addition to describing how U.S. forces and agencies should work internally, the publication also stresses the importance of multilateral engagement in cyberspace. JP 3-12 states "Through dual involvement in national and multinational security processes, USG leaders integrate national and theater strategic CO planning with the [multinational force] whenever possible. Within the multinational structure, US participants work to ensure objectives and strategy complement US interests and are compatible with US capabilities. Within the US national structure, US participants verify international commitments are reflected in national military strategy and are adequately addressed in strategic guidance for joint planning. Planning with international organizations and NGOs is often necessary, particularly if CO support foreign humanitarian assistance, peace operations, and other stability efforts."

ISG has previously included regional and multilateral engagement guidance for the SPP on matters such as countering illegal, unreported, and unrestricted (IUU) fishing (V. Roy, personal communication, March 22, 2022). This successful model should be expanded to include defensive cybersecurity standards. Of the 16 African nations currently participating in the SPP, only 6 are categorized by ISG as having meaningful cyber engagements through the program (Institute for Security Governance, 2020). Far more nations could likely be engaged on the topic if multilateral regional organizations with existing ties to African militaries are leveraged by the Departments of Defense and State.

Diplomacy, The State Department, and Embassy Coordination

NGB needs to ensure that its personnel are coordinating with the GCCs and State Department/Embassy personnel. The State Department has recently rebranded its Office of the Coordinator for Cyber Issues to the Bureau of Cyberspace and Digital Policy. That office maintains coordinators for geographical regions, which are likely in communication with the relevant GCC and Embassy personnel about building cyberspace capacity in each country.

An important consideration for DoD to keep in mind is that cybersecurity is a whole of society effort, expanding beyond military-to-military engagements. National Guard personnel must be aware of other efforts in country including potential State Department-funded cybersecurity efforts. Internet development is a “multi-stakeholder model” and the militarization of foreign internet governance should be avoided. (E. Vish, personal communication, April 1, 2022)

Pilot Program

OSD and NGB should undertake a pilot program implementing the Cyber SPP-specific changes outlined above. Implementing this program in a poorer, cyber-nascent EUCOM and AFRICOM country and comparing outcomes should reveal important lessons what does or doesn’t work, and how potential improvements can be developed. This program should consist of “A logic framework for the initiative that maps goals and specific, measurable, achievable, relevant/results-oriented, and time-bound objectives to the activities necessary to achieve desired changes” as outlined in DoD Instruction 5132.14 (U.S. Department of Defense, 2017). Assessment and monitoring will be made significantly more effective with clear indicators and milestones. OSD should also supply a “theory of change” and data collection instructions to be managed through NGB and sent to the states.

Conclusion

OUSDP can best maximize the effectiveness of the State Partnership Program by engaging with National Guard Bureau to make the most use out of existing or contracted personnel, create a robust assessment, monitoring, and evaluation (AM&E) system, and to standardize engagement with existing lines of effort (LOEs) involving the relevant GEOCOCOMs and U.S. Embassies. Furthermore, establishing forward-leaning relationships with multilateral organizations will help establish more robust cyber capabilities in intended regions and multiply the effectiveness of SPP engagements beyond one country’s borders.

OUSDP should also promote transparency and accountability by moving towards publishing unclassified summaries that can be shared with Congress, academic, think tanks, and the public at large. Robust investment now in developing areas of the world, such as major African nations, will pay dividends later when our partners are more secure and more enveloped in U.S.-style internet governance than the kind advanced by our authoritarian rivals.

References

Ajijola, A.-H., & Allen, N. (2022, March 8). African Lessons in Cyber Strategy. *Africa Center for Strategic Studies*. https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/

Ali, I., & Brice, M. (2020, June 11). What was the cost for the National Guard to deploy in D.C.? Up to $2.6 million a day. *Reuters*. https://www.reuters.com/article/us-minneapolis-police-washington-militar-idUSKBN23I3FP

Allen, N. (2021, January 19). Africa's Evolving Cyber Threats. *Africa Center for Strategic Studies*. https://africacenter.org/spotlight/africa-evolving-cyber-threats/

Allen, N. (2021, November 2). *Email with Dr. Nathaniel Allen, National Defense University* [Email].

Barabanov, I., & Ibrahim, N. (2021, August 11). Wagner: Scale of Russian mercenary mission in Libya exposed. *BBC News*. https://www.bbc.com/news/world-africa-58009514

Bender, B., & McLeary, P. (2021, August 13). *The $88 billion gamble on the Afghan army that's going up in smoke*. POLITICO. https://www.politico.com/news/2021/08/13/afghan-army-pentagon-504469

Borghard, E., & Zabierek, L. (2021, August 18). *What Is Cyber Command's Role in Combating Ransomware?* Lawfare. https://www.lawfareblog.com/what-cyber-commands-role-combating-ransomware

Brooks, C. (2021, February 7). *Cybersecurity Threats: The Daunting Challenge Of Securing The Internet Of Things*. Forbes.

https://www.forbes.com/sites/chuckbrooks/2021/02/07/cybersecurity-threats-the-daunting-challenge-of-securing-the-internet-of-things/

Burgess, M. (2018, February 16). What is the Internet of Things? WIRED explains. *Wired UK*. https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot

Chinese phones with built-in malware sold in Africa. (2020, August 25). *BBC News*. https://www.bbc.com/news/technology-53903436

Clifford, C. (2021, August 31). *Russia's efforts to promote cyber norms that serve its interests gain traction in Africa*. Africa Portal. https://www.africaportal.org/features/russias-efforts-to-promote-cyber-norms-that-serve-its-interests-gain-traction-in-africa/

Crichton, D., & Tabatabai, A. (2018, October 2). NYC wants to build a cyber army. *TechCrunch*. https://social.techcrunch.com/2018/10/02/nyc-wants-to-build-a-cyber-army/

Dixon, W., & Balson, D. (2020, April 2). *COVID-19 shows the urgent need to address the cyber poverty gap*. World Economic Forum. https://www.weforum.org/agenda/2020/03/covid-19-pandemic-shows-the-urgency-for-addressing-the-cyber-poverty-gap/

Douglis, S. (2021, December 15). *The growing discontent within the National Guard: The Indicator from Planet Money*. NPR.Org. https://www.npr.org/2021/12/15/1064679135/the-growing-discontent-within-the-national-guard

Garamone, J. (2022, March 21). *Ukraine-California ties show worth of National Guard program*. National Guard.

https://www.nationalguard.mil/News/Article/2972128/ukraine-california-ties-show-worth-of-national-guard-program/

GCN Staff. (2021, June 21). *States rely on National Guard cyber units*. GCN. https://gcn.com/cybersecurity/2021/06/states-rely-on-national-guard-cyber-units/315478/

Gibbons-Neff, T. (2019, December 20). The Lies the Generals Told About Afghanistan. *The New York Times*. https://www.nytimes.com/2019/12/20/magazine/lies-generals-afghanistan.html

Gibbons-Neff, T., Cooper, H., & Schmitt, E. (2021, June 19). Departure of U.S. Contractors Poses Myriad Problems for Afghan Military. *The New York Times*. https://www.nytimes.com/2021/06/19/world/asia/Afghanistan-withdrawal-contractors.html

Griffiths, R. J. (2016). *U.S. Security Cooperation with Africa: Political and Policy Challenges* (1st edition). Routledge.

Grossman, S., Bush, D., & DiResta, R. (2019). *Evidence of Russia-Linked Influence Operations in Africa*. https://cyber.fsi.stanford.edu/io/publication/evidence-russia-linked-influence-operations-africa

GSMA Staff. (2021). Sub-Saharan Africa. *The Mobile Economy*. https://www.gsma.com/mobileeconomy/sub-saharan-africa/

Hillman, J. E., & McCalpin, M. (2021, May 17). *Huawei's Global Cloud Strategy*. CSIS Reconnecting Asia Project. https://reconasia.csis.org/huawei-global-cloud-strategy/

Institute for Security Governance. (2020). *Cyberspace Capacity Building Playbook*. U.S. Department of Defense.

INTERPOL. (2020). *Online crime in Africa a bigger threat than ever before, INTERPOL report warns*. INTERPOL. https://www.interpol.int/en/News-and-Events/News/2020/Online-crime-in-Africa-a-bigger-threat-than-ever-before-INTERPOL-report-warns

Kadiri, G., & Tilouine, J. (2018, January 26). A Addis-Abeba, le siège de l'Union africaine espionné par Pékin. *Le Monde.Fr*. https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html

Kapp, L., & Serafino, N. M. (2011). *The National Guard State Partnership Program: Background, Issues, and Options for Congress*. 31.

Kheel, R. (2021, May 13). Army secretary nominee concerned about 'unreasonable or unhelpful demands' on National Guard. *The Hill*. https://thehill.com/policy/defense/553401-army-secretary-nominee-concerned-about-unreasonable-or-unhelpful-demands-on/

Kingsley, M. (2022, January 28). *Maria Kingsley Interview* [Phone].

Legato, P., & Mazza, R. M. (2017). Modeling And Simulation Of Cooperation And Learning In Cyber Security Defense Teams. *ECMS 2017 Proceedings Edited by Zita Zoltay Paprika, Péter Horák, Kata Váradi, Péter Tamás Zwierczyk, Ágnes Vidovics-Dancs, János Péter Rádics*, 502–509. https://doi.org/10.7148/2017-0502

Li, J. J., & Daugherty, L. (2015). *Training Cyber Warriors: What Can Be Learned from Defense Language Training?* RAND Corporation. https://www.rand.org/pubs/research_reports/RR476.html

Living below the cyber poverty line: Strategic challenges for Africa. (2022, July 22). The Red Cross.

https://www.redcross.org.tw/english/home.jsp?pageno=201402140002&acttype=view&dataserno=202007220001

Marks, J. (2021, October 26). *The U.S. cyber workforce gap is getting bigger—The Washington Post*. The Washington Post. https://www.washingtonpost.com/politics/2021/10/26/us-cyber-workforce-gap-is-getting-bigger/

McCarthy, J. (2021, August 6). 4 Things To Know After The Philippines Kept Its Pact With The U.S. Military. *NPR*. https://www.npr.org/2021/08/06/1025287447/philippines-united-states-military-agreement-analysis

McLaughlin, J. (2019, July 2). *How Europe's smallest nations are battling Russia's cyberattacks | Heinrich Böll Stiftung | Washington, DC Office—USA, Canada, Global Dialogue*. Heinrich-Böll-Stiftung. https://us.boell.org/index.php/en/2019/07/02/how-europes-smallest-nations-are-battling-russias-cyberattacks

Morgan, S. (2020, November 13). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Mureithi, C. (2021, March 30). *Africa continues to be the global leader in mobile money services*. Quartz. https://qz.com/africa/1990532/africa-continues-to-be-the-global-leader-in-mobile-money-services/

Nakasone, P. (2019, February 14). *Nakasone_02-14-19.pdf*. United States Senate. https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf

Nemec, S. (2021, June 18). *A first of its kind, Adriatic Thunder*. Www.Army.Mil. https://www.army.mil/article/247678/a_first_of_its_kind_adriatic_thunder

Obura, K. (2017, February 28). *Is cyberspace the latest conflict frontier on the African continent?* The Conversation. http://theconversation.com/is-cyberspace-the-latest-conflict-frontier-on-the-african-continent-73496

Odonkor, A. (2020, October 27). *Unveiling the cost of cybercrime in Africa*. CGTN. https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html

O'Flaherty, K. (2018, November 6). *The Nigerian Cyber Warfare Command: Waging War In Cyberspace*. Forbes. https://www.forbes.com/sites/kateoflahertyuk/2018/11/26/the-nigerian-cyber-warfare-command-waging-war-in-cyberspace/

O'Mahony, A., Blum, I., Armenta, G., Burger, N. E., Mendelsohn, J., McNerney, M. J., Popper, S. W., Marquis, J. P., & Szayna, T. S. (2018). *Assessing, Monitoring, and Evaluating Army Security Cooperation: A Framework for Implementation*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2165.html

Pomerleau, M. (2021, December 29). *New US Army cyber unit is building concepts for tactical cyber operations*. C4ISRNet. https://www.c4isrnet.com/cyber/2021/12/29/new-us-army-cyber-unit-is-building-concepts-for-tactical-cyber-operations/

Pros & Cons of Open Source in Business. (2018, March 26). *PDF Blog | Investintech PDF Solutions*. https://www.investintech.com/resources/blog/archives/7975-pros-cons-open-source-business.html

RAND Corporation. (n.d.). *Cyber Warfare*. RAND Corporation. Retrieved September 18, 2021, from https://www.rand.org/topics/cyber-warfare.html

Reilly, L. (2021, June 22). The rising cost of being in the National Guard: Reservists and guardsmen are twice as likely to be hungry as other American groups. *Washington Post*. https://www.washingtonpost.com/business/2021/06/22/hunger-national-guard-reserves/

Roy, V. (2022, March 22). *Conversation with Dr. Vinothini Roy of the Institute for Security Governance* [Personal communication].

Saleh, M. (2021, October 21). *North Africa: Mobile broadband subscriptions by country*. Statista. https://www.statista.com/statistics/1269203/share-of-people-with-active-mobile-broadband-subscriptions-in-north-africa-by-country/

Schaffer, A. (2022, April 4). Analysis | It's a big day at the State Department for U.S. cyberdiplomacy. *Washington Post*. https://www.washingtonpost.com/politics/2022/04/04/its-big-day-state-department-us-cyberdiplomacy/

Schepens, W. J., Ragsdale, D. J., & Surdu, J. R. (2002). *THE CYBER DEFENSE EXERCISE: AN EVALUATION OF THE EFFECTIVENESS OF INFORMATION ASSURANCE EDUCATION*. 15.

Scott, M. (2020, June 1). *Russia and China target U.S. protests on social media*. POLITICO. https://www.politico.com/news/2020/06/01/russia-and-china-target-us-protests-on-social-media-294315

Smith, A. (2018, May 14). *National Guard conducts annual cyber exercise*. National Guard. https://www.nationalguard.mil/News/Article/1520182/national-guard-conducts-annual-cyber-exercise/

St. Laurent, J. A. (2013). *Building Partner Capacity: Key Practices to Effectively Manage Department of Defense Efforts to Promote Security Cooperation*. GOVERNMENT ACCOUNTABILITY OFFICE WASHINGTON DC. https://apps.dtic.mil/sti/citations/ADA573735

State Partnership Program—The National Guard. (2022, January). US National Guard. https://www.nationalguard.mil/leadership/joint-staff/j-5/international-affairs-division/state-partnership-program/

The Joint Staff. (2017, May 23). *Joint Publication 3-20: Security Cooperation*. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_20_20172305.pdf

The White House. (2018, September). *National Cyber Strategy*. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

The White House. (2021, March 3). *Interim National Security Strategic Guidance*. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/03/interim-national-security-strategic-guidance/

Trares, R. (2022, March 31). Indiana National Guard working with Slovakia to help Ukrainian refugees. *Daily Journal*. https://dailyjournal.net/2022/03/31/indiana-national-guard-working-with-slovakia-to-help-ukrainian-refugees/

Tucker, E. (2021, July 19). *Microsoft Exchange hack caused by China, US and allies say*. NPR.Org. https://apnews.com/article/microsoft-exchange-hack-biden-china-d533f5361cbc3374fdea58d3fb059f35

U.S. Department of Defense. (2017, January 13). *DoD Instruction 5132.14—Assessment, Monitoring, and Evaluation policy for the security cooperation enterprise*. DoD Open Government.

https://open.defense.gov/portals/23/documents/foreignasst/dodi_513214_on_am&e.pdf

U.S. Department of Defense. (2018a, September 18). *DoD Cyber Strategy Summary*. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

U.S. Department of Defense. (2018b, October). *National Defense Strategy*. U.S. Department of Defense. https://www.defense.gov/Explore/Spotlight/National-Defense-Strategy/

Van Eerden, J. R. R. (2020). Seeking Alpha in the Security Cooperation Enterprise: A New Approach to Assessments and Evaluations. *Journal of Advanced Military Studies*, *11*(1), 113–126. https://doi.org/10.21140/mcuj.2020110105

Vish, E. (2022, April 1). *Elizabeth Vish Interview* [Phone].

Whitlock, C. (2019, December 9). *Confidential documents reveal U.S. officials failed to tell the truth about the war in Afghanistan*. Washington Post. https://www.washingtonpost.com/graphics/2019/investigations/afghanistan-papers/afghanistan-war-confidential-documents/

Womack, Ruppersberger Request GAO Review of National Guard State Partnership Program. (2020, September 14). Internal | Congressman Steve Womack. http://womack.house.gov/news/documentsingle.aspx?DocumentID=404206

Work, J. (2020). Evaluating Commercial Cyber Intelligence Activity. *International Journal of Intelligence and CounterIntelligence*, *33*(2), 278–308. https://doi.org/10.1080/08850607.2019.1690877

Zhou, W. (2019, April 8). *Languages other than English are encouraged for BRI ties*. China Daily.

https://www.chinadaily.com.cn/a/201904/08/WS5caa8942a3104842260b4c29.

html

Appendix

National Guard service member deployment cost: Washington Post report referring to DC National Guard reply of $530 per servicemember per working day in 2020.

Contracted cost:
McKinsey Report using DoD payroll records, average Army contractor cost $189,188 in 2015. Divide by 260 working days = $727.65 per working day in 2015. Inflation calculator from 2015 to 2020 (matching WaPo report) equals $794.56 per contractor per working day in 2020.