Weekly Media Report – January 18-24 , 2022

EDUCATION:

Navy Cryptologic Warfare Officers Cannot Do Cyber

(USNI Jan 22) … Lt. Cmdr. Derek S. Bernsen

Navy cyber is a ship without a rudder. While every other service has one cyber designator, the Navy's cyber expertise resides in three separate communities. As a result, the three communities are each plagued with unnecessary problems, and none are fully empowered or capable of leading the domain. To solve this issue, the Navy must consolidate responsibility for cyber, invest in the cyber warfare engineer community, and require deep technical experience for all cyber roles… Often, CWOs are deemed cyber experts and put in charge of Cyber Mission Force teams after a single course at the **Naval Postgraduate School** (NPS) in Monterey, California, or a one-month basic course in Pensacola, Florida. A cyber expert must be able to solve hard technical problems related to computer security with minimal support because they understand the underlying technology and have sufficient breadth and depth in the many subfields of cyber. Cyber is far larger than many realize: cryptography, forensics, vulnerability research, penetration testing, exploitation, (cyber) operations, steganography, malware, cyber-threat intelligence, reverse engineering, networking, and development (including exploits, payloads, and effects). Given all their information warfare missions, that CWOs can also become cyber experts is a fallacy. Even with NPS's cyber systems and operations master's degree, CWOs without several years of focused work in technical cyber areas are nothing more than cyber dilettantes.

RESEARCH:

NPS Student's Award-Winning Thesis Helps Naval Station Newport Prepare for Hurricane

(Navy.mil 20 Jan 22) … Rebecca Hoag

(NPS.edu 20 Jan 22) … Rebecca Hoag

When an extreme weather event hits, emergency preparation and procedures get put to the test, and so does the cohesion of multiple areas' evacuation plans. A lack of communication between cities, or between military bases and their local communities, can result in less road accessibility than either party planned for and less room in shelters than anticipated.

FACULTY:

Reviving the Victory Garden: The Military Benefits of Sustainable Farming

(War on the Rocks 20 Jan 22) … Leo Blanken and Ben Cohen

"Uncle Sam Says: Garden." If Americans are familiar with victory gardens, it is probably from old World War I and World War II posters with slogans like this exhorting citizens to participate in the war effort by growing their own vegetables. Today, however, a new strategic campaign is beginning to get underway. In its recent Climate Adaptation Plan, the Department of Defense called for "adaptation," "resilience," and "mitigation" to address the growing national security threat posed by climate change. Modernized victory gardens can play a valuable role in advancing all of these goals… Leo Blanken is an associate professor in the Defense Analysis Department at the **Naval Postgraduate School**, where he also serves as the deputy director of the Consortium for Robotics and

Unmanned Systems Education and Research (CRUSER) and as the academic lead for the Applied Design for Innovation program. He is the author of Rational Empires: Institutional Incentives and Imperial Expansion and is co-editor of Assessing War: The Challenge of Measuring Success and Failure. He also collects and DJs rare funk and soul records from the 1960s.

How the Biden Administration is Making Gains in an Uphill Battle Against Russian Hackers

(The Conversation 21 Jan 22) … Scott Jasper
(Yahoo! News 21 Jan 22) … Scott Jasper

On Jan. 14, 2022, the FSB, Russia's domestic intelligence service, announced that it had broken up the notorious Russia-based REvil ransomware criminal organization. The FSB said the actions were taken in response to a request from U.S. authorities. The move marks a dramatic shift in Russia's response to criminal cyberattacks launched against U.S. targets from within Russia, and comes at a time of heightened tensions between the two countries…Scott Jasper, CAPT, USN (ret) is a Senior Lecturer at the National Security Affairs Department at the **Naval Postgraduate School**, specializing in defense strategy, hybrid warfare, and cyber policy. He is regularly engaged by the DSCA Institute for Security Governance to provide support to foreign governments.

ALUMNI:

President Biden Announces Key Regional Appointments for USDA, FEMA, and HUD

(The White House 20 Jan 22)

Today, President Joe Biden appointed the following individuals to serve in key regional leadership roles at the United States Department of Agriculture (USDA), the Federal Emergency Management Agency (FEMA) at the Department of Homeland Security, and the Department of Housing and Urban Development (HUD)… Nancy Dragani has more than 26 years of experience in the emergency management field at state and federal levels. She began her career with the Ohio Emergency Management Agency in 1994; in 2005 she was appointed the executive director, a role she filled until 2014. Dragani was appointed as the Federal Emergency Management Agency Region 8 Deputy Regional Administrator in January 2016. Her responsibilities included oversight of regional disaster response, recovery, mitigation, and preparedness activities. Dragani also served on FEMA's National Advisory Council and the Memorial Institute for the Prevention of Terrorism Advisory Board. She held the position of President of the National Emergency Management Association (NEMA) from 2008-2009 and was the 2014 recipient of NEMA's Lacy E. Suiter Distinguished Service Award, an annual award to an individual for outstanding contributions to emergency management. Dragani has a Master of Arts from the **Naval Postgraduate School's** Center for Homeland Defense and Security and a Bachelor of Arts degree from Ohio Dominican College where she graduated Summa Cum Laude.

FIU Names Former Head of U.S. Southern Command as Senior Fellow

(Community Newspapers 21 Jan 22)

After a nearly four-decade long career in the military, retired U.S. Navy Adm. Craig S. Faller will join FIU's Steven J. Green School of International & Public Affairs as a senior fellow. He will lecture on national security and leadership, as well as mentor students through the university's intelligence fellowship and global affairs programs… A 1983 graduate of the United States Naval Academy and a native of Fryburg, Pennsylvania, Faller earned a bachelor's degree in systems engineering and a master's in national security affairs from the **Naval Postgraduate School**.

Second GDF officer graduates from U.S. Naval Postgraduate School

(News Room 22 Jan 22)

The U.S. Embassy in Georgetown on Saturday issued a congratulatory message for Colonel Raul Jerrick of the Guyana Defence Force who was successfully awarded a Master of Arts in Security Studies, with an emphasis on Countering Terrorism from the United States **Naval Postgraduate School**.

UPCOMING NEWS & EVENTS:

Jan 25-28: Center for Executive Education SC Workshop
Feb 21: President's Day (Federal Holiday)

EDUCATION:

Navy Cryptologic Warfare Officers Cannot Do Cyber

(USNI Jan 22) … Lt. Cmdr. Derek S. Bernsen

Navy cyber is a ship without a rudder. While every other service has one cyber designator, the Navy's cyber expertise resides in three separate communities. As a result, the three communities are each plagued with unnecessary problems, and none are fully empowered or capable of leading the domain. To solve this issue, the Navy must consolidate responsibility for cyber, invest in the cyber warfare engineer community, and require deep technical experience for all cyber roles.

Leadership and management for Navy cyber is currently divided among cryptologic warfare officers (CWOs), information professionals (IPs), and cyber warfare engineers (CWEs). CWOs are ostensibly responsible for offensive and defensive cyber operations, IPs for operating the information technology systems, and CWEs for the technical engineering work that enables cyber operations (e.g. conducting vulnerability research, exploit and capability development). This model may appear reasonable to those not versed in cyber operations, but it significantly inhibits the service from realizing a potent cyber warfighting capability.

CWOs are spread too thin—forced to juggle five different areas of expertise without the focus or depth each requires. IPs have some technical depth but not enough for the more intricate cyber defense tasks, such as malware reverse engineering. CWEs have the expertise to do everything cyber, but are too few in number (currently only 68 personnel). Because of this division of responsibility, major decisions regarding cyber are made by individuals without technical expertise, and these communities are not aligned to capture the value each brings.

Navy cyber also suffers from undervaluation and apathy. Navy leaders hold a misconception that cyber is a purely joint endeavor from which the Navy receives no benefit. Yet each service has specific uses for cyber professionals and the Navy has done little to invest in maritime cyber. This undervaluation creates a negative feedback loop exacerbated by a lack of demonstrated benefit from the CWO community. Continuing to allow responsibility for cyber to be fragmented will turn this misconception into reality. If the Navy continues down its current path, it will have nothing to contribute to the cyber fight in the next war.

Cryptologic Warfare Officers Cannot Do Cyber, Too

The CWO community (roughly 900 officers), the de facto primary cyber community, also provides expertise for signals intelligence and all information operation missions (electronic warfare, operational security, military deception, and military information support operations). It is difficult enough for one officer community to develop expertise in each of these missions, let adding the cyber mission. CWO community leaders have failed to grasp both the importance and the unique requirements of cyber warfare, resulting in no path to develop cyber experts within their ranks and causing cyber to be undervalued.

Often, CWOs are deemed cyber experts and put in charge of Cyber Mission Force teams after a single course at the **Naval Postgraduate School** (NPS) in Monterey, California, or a one-month basic course in Pensacola, Florida. A cyber expert must be able to solve hard technical problems related to computer security with minimal support because they understand the underlying technology and have sufficient breadth and depth in the many subfields of cyber. Cyber is far larger than many realize: cryptography, forensics, vulnerability research, penetration testing, exploitation, (cyber) operations, steganography, malware, cyber-threat intelligence, reverse engineering, networking, and development (including exploits, payloads, and effects). Given all their information warfare missions, that CWOs can also become cyber experts is a fallacy. Even with NPS's cyber systems and operations master's degree, CWOs without several years of focused work in technical cyber areas are nothing more than cyber dilettantes.

Furthermore, the CWO community does not have a mechanism to screen for technical talent, nor does it

value technical ability. While CWOs claim to value technical talent by encouraging those who apply to have STEM degrees, it is not a requirement nor is knowledge gained in academia put into practice. This is obvious from their published community values.

Needed: A Unified Cyber Warfare Community

The CWO community fails to grasp the scale, potential, and diverse skills within the cyber domain. Seeing it as a unitary skill in which one can get sufficient "cyber-stink" after completing a single assignment at the National Security Agency (NSA), the CWO community continues to undervalue the unique challenges associated with conducting operations, developing capabilities, and managing personnel. Most CWOs view cyber as a black box and not the vast domain it is. Nicolas Chaillan, the Air Force's first chief software officer decried this issue: "Please stop putting a major or [lieutenant colonel] (despite their devotion, exceptional attitude, and culture) in charge [of technical projects affecting millions of users] when they have no previous experience in that field," he wrote. "We would not put a pilot in the cockpit without extensive flight training; why would we expect someone with no IT experience to be close to successful?"

At present, there is no incentive for the CWO and IP communities to develop genuine cyber expertise and viable cyber officer career path, because doing so would require prioritizing cyber above their traditional areas of expertise. Because of this, each community invests far too little into cyber professionalization, which further undervalues cyber. This negative feedback cycle causes the NSA and the other military services to view the Navy as poor performers on all things cyber. Even U.S. Cyber Command recognizes this and does not list Navy CWO as a cyber officer community on its careers page (the Navy enlisted cryptologic technician rating is included).

The CWO and IP communities cannot retain genuine cyber talent, as those officers with the aptitude and desire to be cyber experts feel underused and unappreciated. Why become a cyber expert when your community forces you to continually take unrelated jobs? Even if CWOs with cyber talent were to continue their service, they must check boxes in the five CWO disciplines or risk failing to promote. If they are lucky, they may get a cyber job every third or fourth tour, for a total of two or three tours in a 25–30-year career.

Apparently, the CWO community failed to grasp the lessons identified in the book Range—sample and gain diverse experience in the first few years of a career, then specialize for excellence, not dabble in various things forever. The Army, Air Force, and Marine Corps do not ask their officers to be cyber professionals on a part-time basis, instead devoting large communities (the Air Force has nearly 3,000 cyber officers) to the problem and structuring career paths around creating cyber leaders. These services do not have cyber officer career paths that involve random assignments in infantry battalions or aircraft maintenance squadrons just so their officers can experience "the real military." Yet, the Navy's CWO community does just that.

According to the Secretary of the Navy's March 2019 Cybersecurity Readiness Review, the Navy's "culture, processes, structure, and resources are ill-suited for this new era" and that "a real appreciation of the cyber threat continues to be absent from the fabric of [Navy] culture." The Navy frequently talks about the importance of cyber, but its actions clearly do not match its words. CWOs should not be the ones making decisions about cyberspace, and its lack of cyber expertise has failed to prepare the Navy for many incidents. For example, the creation of the Navy's Cybersecurity Task Force and Operation Rolling Tide after Iranian hackers were already in Navy networks.

Empower the Cyber Warfare Engineer Community

The cyber warfare engineer community was created as the home of the true cyber experts. Unfortunately, the CWEs face many challenges that the other communities are unwilling to help resolve. The CWE community currently is small and does not have the manpower to take on the entire cyber mission, nor does it have billets in some of the most important cyber jobs in the Navy. Most CWE billets are at Navy Cyber Warfare Development Group in Suitland, Maryland, and at NSA up the road. The

CWE community thus far has failed to obtain billets at numerous Navy and Joint commands. Growing a community in a zero-sum Department of Defense (DoD) manpower environment is a slow, cumbersome process, and with few exceptions conversion means taking billets from other communities, something no community in the Navy is keen to allow, even when billets go unfilled for years.

What makes the CWE community capable in cyberspace is its focus on developing deep technical expertise. CWEs have major advantages over other communities for accession thanks to the technical interview process and strict STEM degree requirements. To be competitive, applicants must already have deep technical expertise in security. Candidates compete in a 48-hour capture-the-flag screener, followed by challenging programming assignments, and, finally, a rigorous technical interview. Once in the community, CWEs are sent through a grueling six-month training pipeline in which failure is not tolerated. This is like the Navy's Basic Underwater Demolition/SEAL (BUD/S) training or Navy Nuclear Power school, only for hackers. Only top talent is selected, with less than 30 percent of applicants screening positively in the capture-the-flag event and less than 40 percent passing the interview. This leads to more than 95 percent of CWEs completing the training pipeline, significantly better than what Navy civilians and enlisted cryptologic technician–network (CTN) developers achieve.

Aside from rigorous screening and training, CWEs have more in common with SEALs than is readily apparent. Like SEALs, CWEs are required to become proficient in a wide range of cyber skills allowing them to do what others cannot. CWEs possess the skills to develop the most cutting-edge offensive and defensive cyber capabilities, similar to those required to win a competition like the Zero Day Initiative's Pwn2Own competition. China takes Pwn2Own and its own competition, the Tianfu Cup, seriously as a show of force.

No matter where the nation and DoD go regarding building a cyber force, the Navy will always need its own cyber professionals to operate from and defend naval platforms and target maritime adversaries. The CWEs are the only community that has the requisite technical depth, experience, and focus to lead in cyberspace.

The ultimate solution for the Navy will be to turn over full responsibility for the cyber domain to the CWEs—a course of action that will benefit not just the three communities currently involved, but the entire service. CWEs will be empowered to grow, lead, and provide domain superiority. The CWOs will be freed to focus on their traditional areas of expertise. If the IPs continue to expand their own defensive role in cyber operations, the CWE community will not need to grow to the same scale as the Air Force or Army's cyber officer communities, but it certainly will need more than 1,000 CWEs. This would allow the Navy to not only become a top tier remote cyber operations organization, but to integrate CWEs across the fleet and with Naval Special Warfare, in addition to providing direct support to the fleet when needed.

Empowering the CWEs with full control of the cyber domain also will go a long way in improving retention, resolving billeting issues, and creating more opportunities for impact. But it is an incomplete solution. Empowering also must involve other actions to attract and retain high performers with some of the most in-demand skills in one of the most in-demand industries in the world. There currently are no incentives, bonus pay, or accession bonus options that can be offered to CWEs. As NSA has repeatedly learned, it needs skilled cyber people more than those people need NSA. The same is true for the Navy. NSA has created numerous special pay bands and incentive programs to retain personnel. The Army recognizes the importance of technical leaders and offers software developers and cyber personnel its maximum retention bonus and proficiency pay. The Navy should provide bonus pay for proficiency in programming languages, special duty pay, better career opportunities, and establish a CWE reserve component.

Adversary nations are on near-equal footing in cyberspace and cyber provides a mechanism for outsized impact, even to those that are less sophisticated. The Navy cannot keep untrained and unfocused CWOs operating in this domain. The impact of well-trained CWEs, focused cyber experts, will always be greater than CWOs with only a basic understanding of cyber. Removing cryptologic warfare officers from the cyber domain is a critical move the Navy must take.

Empowering the community that has the intense screening process, deeply technical expertise, and focus on the cyber domain is the only way the Navy can regain its cyber footing. No amount of time in

roles that claim to be cyber but provide little technical depth will change the fact that the Navy currently has unqualified personnel in every cyber role. This problem is solvable, but it requires a major restructuring of responsibility for the cyber domain and requires the Navy to put its money and effort where its mouth is and take cyber seriously.

Navy Cryptologic Warfare Officers Cannot Do Cyber | Proceedings - January 2022 Vol. 148/1/1,427 (usni.org)

Return to Index

RESEARCH:

NPS Student's Award-Winning Thesis Helps Naval Station Newport Prepare for Hurricane

(Navy.mil 20 Jan 22) … Rebecca Hoag
(NPS.edu 20 Jan 22) … Rebecca Hoag

When an extreme weather event hits, emergency preparation and procedures get put to the test, and so does the cohesion of multiple areas' evacuation plans. A lack of communication between cities, or between military bases and their local communities, can result in less road accessibility than either party planned for and less room in shelters than anticipated.

To avoid these kinds of scenarios from happening, the DOD Office of Economic Adjustment, renamed the Office of Local Defense Community Cooperation in 2021, awarded a grant to the City of Newport on Aquidneck Island in Rhode Island, and its resident naval base, to develop coastal resilience plans in collaboration with Naval Station (NAVSTA) Newport, the U.S. Naval War College, and University of Rhode Island. The 18-month Military Installation Resilience Review (MIRR) was led by University of Rhode Island Professor of Marine Affairs Dr. Austin Becker.

Around the time the grant was presented, U.S. Navy Lt. Cmdr. Amanda Jones was looking for a thesis topic to complete her Naval Postgraduate School (NPS) master's degree in Operations Research (OR). She wanted her thesis topic to be useful to people both in and out of the Navy, having worked in logistics and humanitarian planning for the Federal Emergency Management Agency (FEMA) before coming to NPS.

After speaking with a colleague who did his thesis on hurricane preparation in the U.S. Virgin Islands with Dr. Daniel Eisenberg, Assistant Professor of Operations Research at NPS, and Deputy Director for the university's Center for Infrastructure Defense (CID), and Dr. David Alderson, Professor of Operations Research and Director of the CID, she felt doing something similar was the right fit for her. Eisenberg directed her focus towards collaborating with the Newport MIRR effort.

As it turned out, the Jones' work on the installation resilience review ended up being applicable much sooner than anyone anticipated when Hurricane Henri threatened the area in August of 2021, the first storm to make landfall in Rhode Island in 20 years. Suddenly, Jones, Alderson and Becker's team found themselves informing the Newport base on best evacuation and preparation procedures before Jones' thesis was even published.

"Dr. Alderson reached out and next thing I knew, it's Friday night at like 11:00, and he and I are running the model and making a PowerPoint slide and brief, trying to interpret data to provide the emergency responders at the Navy base data for them to brief to the base [commanding officer] on Saturday morning about what might happen if the base has to evacuate," Jones recalls. "It was very satisfying to be able to see my thesis, that wasn't even done yet, was actually able to immediately be used in a real-life scenario."

"Working with students to solve important, real problems is the most rewarding thing we do at NPS, particularly when we can have immediate impact on operations," Alderson added.

Jones' impressive work was presented with the Chief of Naval Operations Award in Operations Research … Her thesis was published in Sept. 2021.

"I've had other students who have done award-worthy work, but Amanda's project is the first one I've seen being used operationally before she even graduates," Eisenberg said.

Jones' project was part of a broader effort called the Critical Infrastructure Resilience Collaboration and Assessment (CIRCA), which is funded by the Office of the Secretary of Defense (OSD) Strategic Environmental Research and Development Program (SERDP). The project's goal is to develop methods that measure worst-case disruptions across independent infrastructure systems on DOD military installations and to create models that support DOD infrastructure planning and management.

The need for this work has increased as the potential for extreme weather events increases. For Rhode Island specifically, recent studies suggest the latitudinal range of tropical cyclones is expanding poleward in warming climates, suggesting instances like Hurricane Henri could become more common at Naval Station Newport.

For her thesis, Jones focused on how well the Aquidneck Island's transportation infrastructure system and designated evacuation shelters could manage mass departures of populations located in flood or evacuation zones. To do this, she produced a time-phased network flow model out of data on population sizes, flooding information, possible routes, and previous evacuation scenarios to measure optimal evacuation times.

She says the most challenging part of the project was building the computer code to run the model, but she was grateful most of the data sets she found were relatively complete and could be used immediately.

Jones considers her work part of the foundation for Rhode Island's evacuation modeling, and she hopes future students can build on it to incorporate true time phase data that accounts for sea-level rise and accurate storm surge data. She said she's already been contacted by another OR student who might continue her work.

Since graduating from NPS, Jones is putting her operations research skills to use, assigned to the Navy Supply Systems Command (NAVSUP) headquarters as an operations research analyst.

NPS Student's Award-Winning Thesis Helps Naval Station Newport Prepare for Hurricane > United States Navy > News-Stories

Naval Postgraduate School - Naval Postgraduate School (nps.edu)

Return to Index

FACULTY:

Reviving the Victory Garden: The Military Benefits of Sustainable Farming

(War on the Rocks 20 Jan 22) … Leo Blanken and Ben Cohen

"Uncle Sam Says: Garden." If Americans are familiar with victory gardens, it is probably from old World War I and World War II posters with slogans like this exhorting citizens to participate in the war effort by growing their own vegetables. Today, however, a new strategic campaign is beginning to get underway. In its recent Climate Adaptation Plan, the Department of Defense called for "adaptation," "resilience," and "mitigation" to address the growing national security threat posed by climate change. Modernized victory gardens can play a valuable role in advancing all of these goals.

Embracing recently pioneered micro-farming techniques can benefit the U.S. military at both the tactical and strategic levels. Specifically, hydroponic container-farming could serve expeditionary operations across the Indo-Pacific and home station units as well. This would ease logistics burdens, provide healthier food for troops in the field, create opportunities to engage partner forces, and generate a fantastic line of strategic branding for the U.S. military in an era of climate change

Gardens at War

Consider the food supply challenges faced in Afghanistan. For two decades, the United States stationed large numbers of troops in this landlocked country, peaking in 2010 at over 100,000 uniformed personnel. These troops required the bulk of their foodstuffs to be transported by ground vehicles via precarious routes through Pakistan. This was not only inordinately costly but left the sustenance of U.S. forces at the whims of an often-capricious ally. The bulk of the food destined for the dining facilities in Afghanistan needed to be "shelf stable" to survive this arduous journey — which came at the cost of it being nutritious (let alone good). One of the authors, for example, spent time at a forward operating base in southern Afghanistan in 2013 where the troops were being fed corn-dogs and canned fruit salad (in heavy syrup!) for multiple days in a row. Even though bad food has been part of soldiers' experience throughout military history, it was no wonder that these particular service members turned to surviving on energy drinks, candy, and protein bars. Finally, the sustainment and logistic system required to move these countless tons of preserved food over thousands of miles generated a massive amount of garbage. Anyone deployed to Afghanistan remembers the smell of the "burn pits" that consumed the mountains of packaging to which the food logistics system contributed.

The major military scenario that is consuming American planners now is a potential conflict spanning the Indo-Pacific. If U.S. forces are deployed across many remote locations and enemy forces have formidable anti-access/area denial capabilities, then sustainment challenges will become paramount. Reducing the required volume of foodstuffs would greatly ease the burden of maintaining a distributed, resilient force posture and could reduce critical vulnerabilities as well. This means the military should consider beginning to research and refine a system of expeditionary micro-farming capabilities to prepare for such an eventuality in the future. How would such food production be implemented within military forces? We can consider the scale and purpose of sustainable agriculture for deployed and home station forces separately.

For deployed units, emerging technology is making it increasingly feasible to operationalize distributed food production in a very real and practical way. Firms within the United States are currently producing "container farms" or "vertical farms" that utilize controlled environment hydroponic or aeroponic techniques to grow food with minimal resources. Built within 8' x 40' containers, these mobile micro-farms may produce as much food as a five-acre farm for leafy-greens and many vegetables. They use 90 percent less water and 80 percent less fertilizer than traditional farming techniques, at the investment cost of roughly $60,000 per container. Depending on the mix of vegetables being grown, this could result in thousands of pounds of produce harvested over each growing cycle. The produce from these farms would be used to provide a healthy supplement to the servicemembers' overall diet, which would still require other sources of protein and carbohydrates, as well as "operational rations" that service members would take with them into combat.

Container farms can be forward deployed with the units that manage them. For example, a Marine Corps combat logistics battalion could maintain container farms at home station and have them ready to ship when needed. Because such container farms can be self-sustaining for 96 hours without water or power, they could be readily deployable, even while growing operations are underway. When paired with alternative energy sources, these containers could support operations in every clime and geographic location, including the Arctic circle. One servicemember, in a common 40-hour work week, could easily manage two containers and distribute the food they produce while still assuming additional duties. That is the equivalent of having a 10-acre farm available for year-round, on demand, food production. Food service and culinary specialists within the military could be rapidly trained on many of these techniques and systems, while earning valuable certifications through the U.S. Department of Agriculture that could serve them in their post-military careers.

A second opportunity for operationalized farming is its potential as a partner force enablement activity. This is not a wholly novel concept. American forces in Afghanistan, for example, utilized farming as a tool to supplant opium production. In this case, however, the sharing of farming techniques and technologies with partners would help to reimagine the potential of security force assistance activities to be more sensitive to the partners' needs while energizing wider engagement with the host nation in an

era of climate-change induced challenges. Further, by synchronizing these activities with other elements of US foreign policy in the partner nation, it would reflect the oft-stated ideal of creating a "whole of government" approach to partner enablement and economic development. This precisely accords with U.S. Agency for International Development's pronouncement that "civilian-military cooperation [is] fundamental to a whole-of-government approach to contemporary national security challenges in keeping with the increasingly important role of development in advancing national security priorities." As many U.S. forces — notably special operations forces — are deployed across the Indo-Pacific, this provides an opportunity for pre-positioning and optimizing distributed micro-farming as an innovative partnering activity. Units such as U.S. Army civil affairs and psychological operations would be particularly well-suited to leverage these activities for strategic impact within the context of great power competition.

For home station food production, the sky is the limit. Military bases in the continental United States have the land and the personnel to engage in significant open air food production activities, in the same way institutions like the Kew Botanical Gardens supported World War-era victory gardens. Some bases, like Fort Bragg and Camp Pendleton, have a plethora of land and personnel that could help transform military food production. This would serve the purpose of providing food for the dining facilities, as well as providing a disciplined, healthy activity that could be folded neatly into other training duties. Further, "regenerative farming" techniques could be used on and near military installations to repair and strengthen topsoil, which is a growing environmental concern. Other bases may have less space, less personnel, and less general training activities. For these locations, farming on base may serve as a recreational opportunity to provide a healthy and widely enjoyed activity for interested personnel. "Morale, Welfare, and Recreation" — the office tasked with promoting the health and resilience of military communities — could coordinate with garrison commanders to provide the space, resources, and time for personnel to maintain and harvest gardens that could supplement the dining facility while improving the quality of life of the men and women in uniform.

Finally, some portion of home-station farming activities could be dedicated to research — done in collaboration with inter-agency partners, academia and industry — to further refine innovative farming techniques for the benefit of all. This public-private partnering to innovate in the face of emerging security challenges is one of the long-standing strengths of the Department of Defense. In such cases, the gains from these collaborations are not only accrued by the military, but can help drive the economy and benefit American society as a whole.

Harvesting the Benefits

A "victory garden" system could be tailored to ease logistics burdens, foster resilience, contribute to health, and serve the Defense Department's messaging on climate change adaptation. These efforts would provide tangible benefits to U.S. national security in a number of ways. First, they would improve sustainability for deployed forces across the Indo-Pacific. Further, as these methods evolve, they could eventually solve additional food sustainment issues for globally distributed American military forces, such as ships at sea, and perhaps even submarines. Second, a "victory garden" system would also provide opportunities to blend distributed food production for American forces into a new assistance activity to engage with partner forces and nations. Third, farming could be implemented by home station units for food production and improved personnel health. Fourth, it would provide opportunities for collaborative research with the private sector, academia, and appropriate inter-agency partners to solve food production challenges for the wider population.

The victory garden system will not single-handedly end climate change. But if executed well and thoughtfully messaged it might help cognitively prepare the Department of Defense for the more fundamental transformations that will be required to address the climate crisis.

Leo Blanken is an associate professor in the Defense Analysis Department at the **Naval Postgraduate School**, where he also serves as the deputy director of the Consortium for Robotics and Unmanned Systems Education and Research (CRUSER) and as the academic lead for the Applied Design for Innovation program. He is the author of Rational Empires: Institutional Incentives and Imperial

Expansion and is co-editor of Assessing War: The Challenge of Measuring Success and Failure. He also collects and DJs rare funk and soul records from the 1960s.

Capt. Ben Cohen is a student at the **Naval Postgraduate School** in the Applied Design for Innovation program. His current research is focused on mobility solutions for Marines in the Arctic. A prior enlisted reconnaissance Marine, he is now a logistics officer with multiple deployments to Indo-Pacific Command and Central Command.

The views expressed in this article are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. government.

Reviving the Victory Garden: The Military Benefits of Sustainable Farming - War on the Rocks

Return to Index

How the Biden Administration is Making Gains in an Uphill Battle Against Russian Hackers

(The Conversation 21 Jan 22) … Scott Jasper
(Yahoo! News 21 Jan 22) … Scott Jasper

On Jan. 14, 2022, the FSB, Russia's domestic intelligence service, announced that it had broken up the notorious Russia-based REvil ransomware criminal organization. The FSB said the actions were taken in response to a request from U.S. authorities. The move marks a dramatic shift in Russia's response to criminal cyberattacks launched against U.S. targets from within Russia, and comes at a time of heightened tensions between the two countries.

U.S. policy and actions in response to cyberattacks connected to Russia have changed distinctly since the Biden administration took office. President Joe Biden has openly confronted Russian President Vladimir Putin on his responsibility regarding international cyberattacks, and the Biden administration has taken unprecedented steps to impose costs on Russian cyber criminals and frustrate their efforts.

Upon taking office, Biden immediately faced difficult challenges from Russian intelligence operatives and criminals in headline-grabbing cyberattacks on private companies and critical infrastructure. As a scholar of Russian cyber operations, I see that the administration has made significant progress in responding to Russian cyber aggression, but I also have clear expectations about what national cyber defense can and can't do.

Software supply chain compromise

The SolarWinds hack carried out in 2020 was a successful attack on the global software supply chain. The hackers used the access they gained to thousands of computers to spy on nine U.S. federal agencies and about 100 private-sector companies. U.S. security agencies said that a sophisticated hacking group, "likely Russian in origin," was responsible for the intelligence-gathering effort.

On Feb. 4, 2021, Biden addressed Putin in a statement delivered at the State Department. Biden said that the days of the U.S. rolling over in the face of Russian cyberattacks and interference in U.S. elections "are over."

Biden vowed to "not hesitate to raise the cost on Russia." The U.S. government had not previously issued indictments or imposed sanctions for cyber espionage, in part out of concerns that they could result in reciprocal actions by Moscow against NSA and CIA hackers. Nevertheless, the U.S. Treasury Department issued sanctions against the Russian Foreign Intelligence Service, the SVR, on April 15, 2021.

Biden also signed an executive order to modernize federal government cybersecurity. He directed agencies to deploy systems that detect cyber incursions, like the one that spotted SolarWinds activity at Palo Alto Networks. In parallel, his security agencies published tools and techniques used by the SVR and ransomware gangs to help organizations defend against them.

Economic sanctions and technical barriers, however, did not slow SVR efforts to gather intelligence on U.S. foreign policy. In May 2021, Microsoft revealed that hackers associated with Russia exploited the mass-mailing service Constant Contact. By masquerading as the U.S. Agency for International Development, they sent authentic-looking emails with links to more than 150 organizations, which, when clicked, inserted a malicious file that allowed computer access.

Ransomware attacks

Also in May, the shutdown of the Colonial Pipeline by a ransomware attack by the Russian cyber gang DarkSide halted the flow of nearly half the gas and jet fuel to the Eastern Seaboard. Panicked drivers rushed to fill up tanks while prices soared. A month later, consumers scrambled to find meat alternatives after REvil infected beef and pork processer JBS USA with ransomware.

Biden said Russia has "some responsibility to deal with this." At a summit in Geneva in June, he handed Putin a list of off-limits critical infrastructure that would merit a U.S. response if attacked. It is likely that Russian intelligence services and law enforcement have a tacit understanding with cybercriminals and can shut down their resources.

Though not counting on Putin to exert influence, the White House formed a ransomware task force to go on the offense against the gangs. The first step was using a counterterrorism program to offer rewards of up to US$10 million for information on hackers behind state-sanctioned breaches of critical infrastructure.

In close collaboration with international partners, the Justice Department announced the arrest of a Ukrainian national in Poland, charged with the REvil ransomware attack against Kaseya, an information technology software supplier. The Justice Department also seized $6.1 million in cryptocurrency from another REvil operator. Romanian authorities arrested two others involved in REvil attacks.

U.S. law enforcement seized $2.3 million paid in ransom to DarkSide by Colonial Pipeline by using a private key to unlock bitcoin. And the Treasury Department disrupted the virtual currency exchanges SUEX and Chatex for laundering the proceeds of ransomware. Treasury Department sanctions blocked all of their property in the U.S. and prohibited U.S. citizens from conducting transactions with them.

Additionally, the top U.S. cyberwarrior, Gen. Paul Nakasone, acknowledged for the first time in public that the U.S. military had taken offensive action against ransomware groups. In October, U.S. Cyber Command blocked the REvil website by redirecting traffic, which prevented the group from extorting victims. After REvil realized its server was compromised, it ceased operations.

Limits of US responses

Russia conducts or condones cyberattacks by state and criminal groups that take advantage of gaps in international law and avoid crossing national security lines. In October, the SVR stepped up attempts to break into technology companies to steal sensitive information. U.S. officials considered the operation to be routine spying. The reality that international law does not prohibit espionage per se prevents U.S. responses that could serve as strong deterrents.

Similarly, after cyber gang BlackMatter carried out a ransomwware attack on an Iowa farm cooperative in September, the gang claimed that the cooperative did not count as critical infrastructure. The gang's claim refers to cyberattack targets that would prompt a national response from the U.S. government.

Despite this ambiguity, the administration has unleashed the military to frustrate the efforts of ransomware groups, while law enforcement agencies have gone after their leaders and their money, and organizations in the U.S. have shored up their information systems defenses.

Though government-controlled hackers might persist, and criminal groups might disappear, rebuild and rebrand, in my view the high costs imposed by the Biden administration could hinder their success. Nevertheless, it's important to bear in mind that national cyber defense is an extremely challenging problem and it's unlikely that the U.S. will be able to eliminate the threat.

Scott Jasper, CAPT, USN (ret) is a Senior Lecturer at the National Security Affairs Department at the **Naval Postgraduate School**, specializing in defense strategy, hybrid warfare, and cyber policy. He is regularly engaged by the DSCA Institute for Security Governance to provide support to foreign governments.

How the Biden administration is making gains in an uphill battle against Russian hackers (theconversation.com)

How the Biden administration is making gains in an uphill battle against Russian hackers (yahoo.com)

Return to Index

ALUMNI:

President Biden Announces Key Regional Appointments for USDA, FEMA, and HUD

(The White House 20 Jan 22)

Today, President Joe Biden appointed the following individuals to serve in key regional leadership roles at the United States Department of Agriculture (USDA), the Federal Emergency Management Agency (FEMA) at the Department of Homeland Security, and the Department of Housing and Urban Development (HUD):

These regional appointees will be critical to the President's efforts to rebuild communities most impacted by the pandemic, the economic recovery, and climate change. They bring deep expertise in their issue areas as well as critical relationships with federal, state, tribal, and local leaders. And, consistent with the President's commitment to building an administration that looks like America, these regional appointees represent the diversity of America and the communities they serve.

UNITED STATES DEPARTMENT OF AGRICULTURE (USDA)

The USDA's Farm Service Agency implements agricultural policy, administers credit and loan programs, and manages conservation, commodity, disaster, and farm marketing programs in each U.S. State. Its mission is to equitably serve all farmers, ranchers, and agricultural partners through the delivery of effective, efficient agricultural programs for all Americans. State Executive Directors oversee this work, ensuring the needs of local constituents are met and that USDA resources are distributed equitably and fairly.

USDA's Rural Development mission area is committed to helping improve the economy and quality of life in rural America. State Directors lead offices that offer grants, loans, and loan guarantees to help create jobs and support economic development and essential services.

C. John Sullivan III, USDA State Executive Director, Farm Service Agency, Maryland

John Sullivan previously served as the Program Manager for the Maryland Department of the Environment (MDE) overseeing the Animal Feeding Operations (AFO), Biosolids, Waste Diversion, and Hazardous Waste Permits divisions. Through the issuance of AFO permits and compliance he also emphasized the importance of a collective relationship between the Maryland Departments of Agriculture and Environmental Protection, and represented MDE on the State Soil Conservation Committee. Prior to this role, Sullivan served as the Deputy Chief of Staff and Agricultural Liaison to the Harford County, Maryland County Executive for the agricultural industry. He developed the first comprehensive agricultural economic development plan for Harford County, received the National Association of Counties Achievement Award for the Ag 2000 initiative and Buy Local Campaign, developed marketing programs to enhance economics of the agricultural industry, and conducted legislative service related to agriculture.

In the 1990s Sullivan served as an Agriculture and Natural Resource Fellow for the U.S. EPA Chesapeake Bay Program in Annapolis, MD and the National Civilian Community Corps in Washington, D.C. He has served as the Past President and is a current board member of the Maryland Agricultural Education Foundation and the Maryland Agricultural Council; is an active member of the Maryland Farm Bureau; is an alumnus of LEAD Maryland and Leadership Maryland; and is a lifetime member of the Maryland Historical Society and the Havre de Grace Decoy Museum. Sullivan lives in Harford County, Maryland on his family's fifth-generation property in Fallston with his wife and three children who are active in the beef and equine industry, 4-H Livestock, the FFA, and agricultural high school magnet programs.

Daniel A. Smiarowski, USDA State Executive Director, Farm Service Agency, Massachusetts

Daniel Smiarowski has worked with the USDA Farmers Home Administration and Farm Service Agency since 1986. He started as a Student Trainee upon graduating from the Stockbridge School of Agriculture where he studied fruit and vegetable crops. He became an Assistant County Supervisor after graduating from the University of Massachusetts with a degree in Agricultural Economics in 1988. Since then, he has served as a Farm Loan Specialist and District Director in the Massachusetts Farm Service Agency for a majority of his career. Over the past 35 years, he has worked with a diverse group of farms in Massachusetts including fruit and vegetables, cranberries, dairy, greenhouse operations, shellfish, and tobacco.

Smiarowski grew up on the 175-acre family farm located in Montague and Sunderland, MA that he currently owns and operates with his wife Penny. He is the third generation to operate the farm, which was started in 1923. The farm has operated as a dairy and a diversified vegetable farm over the years. Smiarowski currently produces asparagus, butternut squash, and pumpkins and leases the remainder of the land to family members and an organic beginning farmer. He has two children, Alexander and Alina.

Steve Kouplen, USDA State Executive Director, Farm Service Agency, Oklahoma

Born and raised on the family farm and ranch near Beggs in east central Oklahoma, Steve Kouplen learned the value of education, graduating from Oklahoma State University with a B.S. and M.S. in Agricultural Education. While raising a family and operating a commercial Hereford cattle ranch and farm, Kouplen served in several county and state leadership roles, including serving as President of the Okmulgee County Farm Bureau and Oklahoma Farm Bureau, Chairman of the Oklahoma Beef Council, and member of the board of directors for the East Central Electric Cooperative, Beggs School District, and Okmulgee County Fair Board. He is also a past member of the local Farm Service Agency Committee and the Okmulgee County Rural Water District #6. Kouplen was elected in 2009 to the Oklahoma House of Representatives and quickly rose through the ranks to Minority Leader.

John Litz, USDA State Executive Director, Farm Service Agency, Tennessee

John Litz is a lifetime farmer in Hamblen County, Tennessee. He was born and raised on his family farm in Morristown that he and his wife Kathy now share. Their farming operation includes 3,000 acres of corn, soybeans, wheat, turf grass, and a vineyard. After graduating from the University of Tennessee, Knoxville, Litz was an owner/manager in a 2500+ head feed lot operation in charge of animal health and assisted with row crop management. Additionally, Litz graduated from the University of Kentucky's 2-year Leadership Program. Litz has received awards for Lancaster Sunbelt Farmer of the Year for the State of Tennessee, Hamblen County Farm Family of the Year, and Hamblen County Agribusiness Person of the Year. He has been involved in organizations such as UT Agriculture Regional Advisory Committee, BPOE (Elks Lodge), Hamblen County Democrat Party, numerous Farm Bureau committees locally and state-wide, and is a member of All Saints' Episcopal Church, Morristown. He served as Vice-Chair of the State Democrat Party and is a member of the State Democrat Executive Committee. Litz also served four terms in the State House of Representatives for Hamblen County where he sat on the Agriculture

Committee, State & Local Government Committee, Election Subcommittee, and was an officer as a freshman on the Calendar and Rules Committee. He was elected as Assistant Democrat Leader while in office. Litz looks forward to serving Tennessee as FSA Executive Director, and he will strive to keep farmers across the state informed about FSA programs.

John Roberts, USDA State Executive Director, Farm Service Agency, Vermont

John Roberts immigrated from Great Britain, after completing his college education with a BS degree in Farm Management, to Vermont in 1974. He managed Shelburne Farms in Shelburne, Vermont for two and a half years until the spring of 1977. At that time, Roberts and his wife Lisa bought a 260-acre farm in Cornwall. Starting with 36 cows, they farmed until 2012 and grew the farm to 400 acres and 195 registered Brown Swiss cows, and raised four children. Following that, Roberts worked for over six years for the Vermont Agency of Agriculture as a water quality specialist. Roberts assumed the position of Executive Director of the Coalition at the beginning of June 2020. Over the years, Roberts has been active in his community as a Select Board member as well as in several state and national committee positions focused on agricultural, conservation, and environmental policy, including the National Beef Board and the Grazing Lands Conservation Initiative. On the state level, Roberts served on the Vermont Water Resources Board, the Vermont Housing Conservation Board, the Board of the Vermont Land Trust, and as Chair of the state USDA-FSA Committee and has been active in rewarding farmers for sound environmental practices.

Jonathan McCracken, USDA State Director, Rural Development, Ohio

Jonathan McCracken serves as a Senior Advisor to U.S. Senator Sherrod Brown (D-OH). For the past 15 years, he has held various legislative positions related to agriculture, rural development, food, nutrition, energy, and environmental policy. McCracken has extensive experience bringing together and working with community leaders, economic development officials, and government agencies on programs benefitting Ohio and its rural communities. Prior to working for Senator Brown, McCracken began his career working for Senator Edward M. Kennedy (D-MA). A native of Wilmington, Ohio, McCracken is a graduate of Wake Forest University and earned a J.D. from the George Washington University Law School. McCracken currently resides with his family in Columbus, Ohio.

Margaret Hoffmann, USDA State Director, Rural Development, Oregon

Margaret Hoffmann has over a decade of experience working on rural economic development in Oregon. Hoffmann has spent the last five years working at the Farmers Conservation Alliance to help over 50% of irrigated agriculture modernize their systems to increase economic resilience and environmental benefits. As the Strategic Operations Manager, she helped raise over $750 million in infrastructure funding to move projects through planning, design, and implementation. Prior to joining the Farmers Conservation Alliance, Hoffmann served as the Energy Policy Advisor to Governors Brown and Kitzhaber. In that role, she coordinated with a broad array of stakeholders to facilitate the state's transition to an economically resilient, lower-carbon future. Hoffmann has a deep understanding of how challenging it can be for people to navigate the complexities of accessing federal assistance She looks forward to leveraging Rural Development's resources to increase equitable access program capital, address climate change, and economically recover from the ramifications of COVID.

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

Regional Administrators lead FEMA's 10 Regional offices and coordinate directly with the FEMA Administrator to support state, local, tribal, and territorial (SLTT) communities in their geographic area of operations delivering frontline services across the spectrum of preparedness, mitigation, response,

recovery, and continuity programs. The Regional Administrators play a critical role in delivering timely, efficient, effective, and accessible federal assistance.

Lori Ehrlich, FEMA Regional Administrator, Region 1

During Lori Ehrlich's 14-year tenure as a Massachusetts State Representative, she served in leadership roles as Chair of the Joint Committee on Municipalities and Regional Government and the Joint Committee on Export Development. She has filed and passed numerous bills into law on topics ranging from clean energy, climate change, and local journalism, to animal protection and reforming restrictive employment contracts. Ehrlich was appointed to serve on a U.S. Department of Energy Commission on Energy Preparedness.

Prior to her elected service, Ehrlich founded two environmental non-profit organizations that brokered both the closure of a 1950s-era coal-burning power plant and the remediation of a contaminated drinking water supply for 80,000 local residents. Ehrlich earned a Master's degree in Public Administration from Harvard University's Kennedy School of Government. She earned a Bachelor's of Science degree in Accounting from Lehigh University and is the only CPA currently serving in the legislature.

Region 1 serves Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont.

David Warrington, FEMA Regional Administrator, Region 2

David Warrington has almost 20 years of experience in the public sector. Most recently he was the Senior Manager of Strategic Preparedness for the Port Authority of New York and New Jersey, where he was responsible for developing an all-hazards risk management program to assess complex threats and lead the evaluation of mitigation strategies. Since 2014, he has led the advancement of next generation technology for the Agency's chemical, biological, and radiological defense efforts. In 2019, he oversaw the review and comprehensive updates to all the Port Authority's emergency operations plans.

Throughout his career Warrington has served in a leadership capacity for all command positions within the Port Authority's incident command structure including responses to Hurricanes Sandy and Irene, U.S. Airways flight 1549 crash into the Hudson River, and numerous named winter storms. Additionally, he had a lead role in coordinating Agency resources to support Super Bowl XLVIII in New Jersey, and the 2015 Papal visit to New York City, both designated National Special Security Events. Warrington received his Bachelor of Arts degree from York College of Pennsylvania with a focus in criminal justice. He currently resides in Jersey City, New Jersey.

Region 2 serves New Jersey, New York, Puerto Rico, and the U.S. Virgin Islands.

Nancy Dragani, FEMA Regional Administrator, Region 8

Nancy Dragani has more than 26 years of experience in the emergency management field at state and federal levels. She began her career with the Ohio Emergency Management Agency in 1994; in 2005 she was appointed the executive director, a role she filled until 2014. Dragani was appointed as the Federal Emergency Management Agency Region 8 Deputy Regional Administrator in January 2016. Her responsibilities included oversight of regional disaster response, recovery, mitigation, and preparedness activities. Dragani also served on FEMA's National Advisory Council and the Memorial Institute for the Prevention of Terrorism Advisory Board. She held the position of President of the National Emergency Management Association (NEMA) from 2008-2009 and was the 2014 recipient of NEMA's Lacy E. Suiter Distinguished Service Award, an annual award to an individual for outstanding contributions to emergency management. Dragani has a Master of Arts from the **Naval Postgraduate School's** Center for Homeland Defense and Security and a Bachelor of Arts degree from Ohio Dominican College where she graduated Summa Cum Laude.

Region 8 serves Colorado, Montana, North Dakota, South Dakota, Utah, and Wyoming.

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT (HUD)

Regional Administrators lead HUD's 10 Regional Offices that directly serve state and local organizations. Regional Administrators oversee field offices across each state in their region and ensure the Department directly serves local communities. Regional Administrators play a key role in leading assignments of housing assistance funds within the region and coordinating those assignments with HUD headquarters.

Alicka Ampry-Samuel, HUD Regional Administrator, Region 2

Alicka Ampry-Samuel served as a member of the New York City Council where she chaired the Public Housing Committee and as Deputy Leader. Her council district represented the highest concentration of public housing in North America. Prior to being elected to the City Council, Ampry-Samuel served on the senior team at the New York City Housing Authority. She has held a number of public service positions, including as a Chief of Staff in the New York State Assembly and working at the United States Embassy in Accra, Ghana as a Democracy and Human Rights Coordinator. Ampry-Samuel has over 20 years of experience helping individuals, families, and organizations in the housing and community development fields.

Region 2 serves New Jersey and New York.

Matthew Heckles, HUD Regional Administrator, Region 3

Matthew Heckles has nearly 20 years of experience working to advance the cause of affordable housing and community development. Heckles served as the Assistant Secretary of the Maryland Department of Housing and Community Development and the Director of the Community Development Administration. In this capacity, he oversaw the operations, administration, and financing of single-family mortgage, multifamily development financing, asset management, rental assistance, energy and weatherization, housing rehabilitation, small business lending, and local government infrastructure programs. Most recently, his work focused on COVID-19 relief programs that provided forbearance for small businesses as well as tenant and homeowner assistance. Prior to his service in Maryland, he worked in various positions at the Delaware State Housing Authority for over 12 years.

Region 3 serves Delaware, Maryland, Pennsylvania, Virginia, West Virginia, and Washington, D.C.

Jose Alvarez, HUD Regional Administrator, Region 4

Jose Alvarez was born in Havana, Cuba and came to the United States as a child. Alvarez is a Licensed Real Estate Broker and a small business owner who has had the privilege of serving his industry and community by taking part in numerous home ownership and business growth initiatives. Among numerous appointments to industry committees and boards, he's served on the Florida Association of Realtors® Board of Directors, the Osceola County Association of Realtors Board of Directors, and in 2009 he was elected to serve as President of the Osceola County Association of Realtors. Throughout Alvarez' 20+ years as a Realtor, he has participated in numerous homeownership initiatives.

In 2012, Alvarez was elected to the Kissimmee City Commission where he championed diversified economic growth, affordable housing and homelessness initiatives, sustainable environmental policies, and fair labor practices. In 2016, he was elected to serve as City of Kissimmee Mayor, becoming the city's first Hispanic Mayor. Over the years, Alvarez has served numerous causes, boards, and committees throughout Osceola County. From multi-million-dollar endeavors to life-changing initiatives, through his various board memberships and affiliations, Alvarez has been responsible for advising CEOs and lawmakers, contributing to strategic plans, approving budgets and business decisions, evaluating management, and representing his charge to stakeholders. Alvarez' true passion is the people he represents. Alvarez and his wife Darlene have been married for 32 years and have five beautiful daughters and five grandchildren.

Region 4 serves Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee, Puerto Rico, and the U.S. Virgin Islands.

Ulysses "Deke" Clayborn, HUD Regional Administrator, Region 7

Ulysses Clayborn is currently the managing member of Clayborn & Associates, LLC, a law firm located in Kansas City, Missouri whose practice is focused in the real estate development area. The firm primarily represents developers and lenders engaged in development of multifamily housing and commercial development projects. Clayborn has experience with projects financed with funds from multiple sources, including multifamily revenue bonds, low-income housing tax credits ("LIHTC"), historic tax credits, and other federal, state, and local funds. He has also provided legal services to clients utilizing HUD financing tools, such as FHA-insured loan programs, Rental Assistance Demonstration (RAD), Choice Neighborhood Initiative and the Risk-Sharing. Clayborn was counsel on one of the first complete portfolio conversion RAD transactions in Missouri. Prior to forming Clayborn & Associates, he served as General Counsel to the Missouri Housing Development Commission ("MHDC"), the state's housing finance agency. There he provided legal services to the MHDC board and staff, including those required to administer the federal LIHTC, state LIHTC, HOME Partnerships, Community Development Block Grant, and other housing programs. These programs provided the financial resources required for the development of thousands of affordable and mixed-income housing units throughout the state of Missouri. Clayborn has served as counsel to the Economic Development Corporation of Kansas City, Missouri, AltCap, an allocator of New Markets Tax Credits, and other entities engaged in commercial and economic development. His first legal position in the real estate area was as a closing attorney for HUD, where he was trained by attorneys possessing an expertise in FHA/HUD programs.

Region 7 serves Iowa, Kansas, Missouri, and Nebraska.

President Biden Announces Key Regional Appointments for USDA, FEMA, and HUD | The White House

Return to Index

FIU Names Former Head of U.S. Southern Command as Senior Fellow

(Community Newspapers 21 Jan 22)

After a nearly four-decade long career in the military, retired U.S. Navy Adm. Craig S. Faller will join FIU's Steven J. Green School of International & Public Affairs as a senior fellow. He will lecture on national security and leadership, as well as mentor students through the university's intelligence fellowship and global affairs programs.

As commander of U.S. Southern Command, Faller, 60, oversaw U.S. military operations in Latin America and the Caribbean from November 2018 until he stepped down in October 2021. At FIU, Faller will work closely with the Jack D. Gordon Institute for Public Policy, as well as the Center for Leadership.

"Admiral Faller has always highlighted the importance of engaging leaders in the Western hemisphere in strategic partnerships and maintaining peace,'' said John F. Stack Jr., founding dean of the Green School. "He has also been a tremendous partner to FIU and the Green School and we are so pleased to have that partnership continue in this new role."

Before joining Southcom, Faller served as senior military assistant to the secretary of defense and held numerous high-level positions at U.S. Pacific Command and U.S. Central Command. He served as a commanding officer in the Persian Gulf War, as well as operations New Dawn in Iraq and Enduring Freedom in Afghanistan.

At FIU, Faller has regularly headlined major events on national security issues including the Hemispheric Security Conference in May 2021, where his roundtable conversation with university leaders drew thousands of online viewers.

"Admiral Faller brings tremendous national security and leadership expertise that will undoubtedly educate and inspire our students while enhancing the quality of FIU's national security-focused research and programming,'' said Brian Fonseca, director of the Gordon Institute, which has had a robust academic partnership with Southcom since 2007.

A 1983 graduate of the United States Naval Academy and a native of Fryburg, Pennsylvania, Faller earned a bachelor's degree in systems engineering and a master's in national security affairs from the **Naval Postgraduate School**.

"I am honored to join the FIU team,'' Faller said after meeting with President Mark B. Rosenberg on Wednesday. "FIU is a world-class organization. As commander of U.S. Southern Command, I saw firsthand the great work FIU does educating students, partnering with the Miami community and building security in our Western Hemisphere neighborhood."

Senior fellows at the Green School devote their residence at FIU to research, teaching and creation of new engagement opportunities for students. Previous fellows include former Miami Mayor Manny Diaz, Kimberly Green of the Green Family Foundation and European historian Peter Reill.

FIU names former head of U.S. Southern Command as senior fellow | Miami's Community News (communitynewspapers.com)

Return to Index

Second GDF officer graduates from U.S. Naval Postgraduate School

(News Room 22 Jan 22)

The U.S. Embassy in Georgetown on Saturday issued a congratulatory message for Colonel Raul Jerrick of the Guyana Defence Force who was successfully awarded a Master of Arts in Security Studies, with an emphasis on Countering Terrorism from the United States **Naval Postgraduate School**.

He is only the second Guyanese officer to graduate from this prestigious institution.

Colonel Jerrick's thesis focused on ideological radicalization. He also studied Defense Capability Development and Innovation and Adaption in the Military, the Embassy said in its statement.

The Naval Postgraduate School, located in Monterey, California, offers over 75 unique academic curricula to military and civilian members of the U.S. Department of Defense and its allies around the world.

Colonel Jerrick's education was funded through the U.S. Government's International Military Education and Training (IMET) program. IMET trains military students throughout the world and builds alliances for the future.

In 2021, IMET funded education for 32 members of the Guyana Defence Force and two members of the Government of Guyana, totaling US$539,000.

The investment is part of the U.S. commitment to Guyana's security.

Second GDF officer graduates from U.S. Naval Postgraduate School – News Room Guyana

Return to Index