2022-02-28

NPS in the News Weekly Media Report - Feb. 22-28, 2022

Naval Postgraduate School (U.S.)

Weekly Media Report – February 22-28, 2022

RESEARCH:

The Navy's New Mine-Hunting Systems Are Major Breakthroughs

(National Interest 24 Feb 22) … Kris Osborn

The U.S. Navy is making fast progress with new countermine technologies to track, identify, and destroy enemy mines… Leading Navy thinkers have been well aware of the threat posed by mines for years, and many have come to believe that mine-hunting capabilities will only become more important. A 2017 report from the **Naval Postgraduate School** identifies five key areas that the Navy must focus on in order to stay in front of the growing mine threat. Interestingly, the areas identified in the essay align very closely with the recent efforts of the Navy and Raytheon. The capabilities that the report identifies as most important "sensor range and resolution, automatic target recognition, and acoustic communications bandwidth" are entirely consistent with the aims of the AQS-20 and Barracuda programs.

No, There Is No 'Woke Military'

(Wonkette 25 Feb 22) … Robyn Pennacchia

Right now, as it concerns Putin's invasion of Ukraine, the American Right is in the "throwing shit up on the wall to see what sticks" phase. For the most part they've landed on a narrative involving Joe Biden cruelly ignoring Vladmir Putin's "legitimate security concerns" by forcing the sovereign nation of Ukraine to join NATO, even though Putin explicitly said he didn't want them to do that, basically forcing him to invade the country and maybe detonate some nuclear weapons on them… PBS reported last year that "numerous studies, including a report last year from the Government Accountability Office, show Black and Hispanic service members were disproportionately investigated and court-martialed. A recent **Naval Postgraduate School** study found that Black Marines were convicted and punished at courts-martial at a rate five times higher than other races across the Marine Corps."

FACULTY:

SWJ Book Review – Understanding Dark Networks: A Strategic Framework for the Use of Social Network Analysis

(Small Wars Journal 24 Feb 22) … Isaac Poritzky

Understanding Dark Networks provides an introduction to Social Network Analysis (SNA), a relatively new, and underutilized research technique that provides a view of dark networks unachievable in traditional lenses. SNA "can be used to gain a greater understanding of dark networks as well as craft strategies that undermine them"

The authors, Daniel Cunningham, Associate Faculty for Instruction at the Common Operational Research Environment (CORE) Lab embedded in the **Naval Postgraduate School**'s Department of Defense Analysis, Sean Everton, Professor in the Department of Defense Analysis and the Co-Director of the CORE Lab, and Philip Murphy, Associate Professor at Middlebury Institute of International Studies at Monterey are experienced scholars who have written extensively on "dark networks" and run the CORE lab, whose mission it is to serve as the leading Department of Defense (DOD) organization in providing research and education to US and foreign military officers

in advanced methodologies and cutting-edge, analytic technologies. SNA is the next essential methodology for DOD analysts, practitioners, and researchers.

New ACM TechBrief Spotlights Privacy, Ethics Problems with Facial Recognition Technology

(EurekAlert 24 Feb 22)

The Association for Computing Machinery's global Technology Policy Council (ACM TPC) today released "ACM TechBrief: Facial Recognition," a concise overview of an increasingly-used application which relies heavily on artificial intelligence. The brief includes a primer on facial recognition, key statistics about its growth and use, as well as important policy implications…"This is an urgent moment," explains Dr. Joshua A. Kroll, an Assistant Professor at the **Naval Postgraduate School** and lead author of the ACM TechBrief. "Articles about facial recognition have been all over the news lately and some of the world's leading companies are fundamentally rethinking whether or not to use the technology. But the public's understanding of the technology, as well as why it is controversial, is vague. The ACM Technology Policy Council developed this overview to familiarize people with the basics of facial recognition, as well as why many computing professionals are concerned about its potential negative impacts. We hope this TechBrief helps frame a public discussion of facial recognition and prevents people from being harmed by these technologies."

How Much Damage Could a Russian Cyberattack do in the US?

(The Chron 25 Feb 22) … Scott Jasper, Naval Postgraduate School
(The Conversation 25 Feb 22) … Scott Jasper, Naval Postgraduate School
(Seattle PI 25 Feb 22) … Scott Jasper, Naval Postgraduate School
(Goskagit 25 Feb 22) … Scott Jasper, Naval Postgraduate School
(Malaysia Sun 25 Feb 22) … Scott Jasper, Naval Postgraduate School

U.S. intelligence analysts have determined that Moscow would consider a cyberattack against the U.S. as the Ukraine crisis grows.

Russia, China, and Iran: The Face of Competition in the Middle East (Podcast)

(MWI 25 Feb 22) … Kyle Atwell and Andrew Milburn

Russia, China, and Iran have all been learning how to conduct irregular warfare from the United States. They model their current irregular warfare approaches based on perceived lessons from observing US interventions in the world over the past few decades, according to arguments put forth in Episode 47 of the Irregular Warfare Podcast… Dr. Seth Jones is senior vice president at the Center for Strategic and International Studies in Washington, DC. He also teaches at Johns Hopkins University and at the US **Naval Postgraduate School**. He is the author of multiple books, to include Three Dangerous Men: Russia, Iran, China and the Rise of Irregular Warfare—which serves as the basis for this conversation.

Putin Just Pushed the World Into an Even Bigger Energy Crisis

(Foreign Policy 28 Feb 22) … Brenda Shaffer, Naval Postgraduate School

Even without sanctions, Russia's war will increase the shortage of oil and gas.

As we approach the 50th anniversary of the 1973 global oil crisis, international energy markets and the global economy are about to receive a similar jolt. Since Russia attacked Ukraine on Feb. 24, the price for crude oil has twice soared as high as $105 a barrel—a level last seen in 2014. And things could get a lot worse from here. Even if the current sanctions imposed on Russia do not explicitly target the energy trade, sanctions on banks and other entities will impede Russia's oil, natural gas, and coal exports, wreaking havoc on global energy markets. In addition, the dangers for oil tankers traveling in the Black Sea will reduce oil reaching global markets, including seaborne supplies from non-Russian producers such as Kazakhstan. The cut in Russian oil and natural gas supplies to markets will have spillover effects and further jack up the prices of coal and liquefied natural gas (LNG), adding another burst to inflation.

What the Trump Administration Brought to the Foreign-Policy Table

(Real Clear Policy 24 Feb 22) … S. Paul Kapur, Naval Postgraduate School

Critics have characterized the Trump administration's foreign policy as chaotic and unsystematic, but it was rooted in three principles that differed from both typical Democratic and Republican positions. Although the administration did not always articulate these principles, by bringing them the Trump team left a lasting impact on

U.S. foreign policy that extends even to Trump's political opponents… S. Paul Kapur is a Professor at the **Naval Postgraduate School** and a visiting fellow at the Hoover Institution. From 2020-2021, he served on the State Department's Policy Planning Staff. The views in this article are his alone.

Russian Cyberattack Risk May Spur US Cybersecurity Investments

(SP Global 25 Feb 22) … David DiMolfetta

The U.S. is preparing for Russian cyberattacks as the conflict between Russia and Ukraine escalates, a fact that may spur cybersecurity spending in the near term… One possible solution would be for companies to implement extended detection and response, or XDR technologies, into their security frameworks in order to protect against threat actors, said Scott Jasper, a senior lecturer at the **Naval Postgraduate School** in Monterey, Calif., and author of Russian Cyber Operations: Coding the Boundaries of Conflict.

ALUMNI:

SPOC Names Timothy R. Jett as Chief Operating Officer

(Trussville Tribune 25 Feb 22)

SPOC welcomes Timothy (Tim) R. Jett as the new Chief Operating Officer (COO)… Jett graduated from the United States Naval Academy, earning his Bachelor's degree in economics; he also holds an MBA in logistics and supply chain management from the **Naval Postgraduate School**. His move back to Alabama is a homecoming of sorts; he grew up in Scottsboro, about two hours northeast of SPOC headquarters.

Compton, Winn to Receive Scouting Award

(The West Alabama Watchman 25 Feb 22)

Rear Adm. Bryan Whitfield Compton Jr. of Demopolis and Luther Winn Jr. of Eutaw are the recipients of the 2022 Hugh A. Lloyd Lifetime Scouting Achievement Award… The admiral has an Associate of Science Degree from Marion Military Institute, a B.S. from the U.S. Naval Academy and an M.S. in Electrical Engineering from the U.S. **Naval Postgraduate School**.

How To Build Leadership Programs For Women In Your Organization

(Global Trade Mag 25 Feb 22) … Barbara Bell

The percentage of women who hold leadership roles in business, higher education and government grows with each passing year – sometimes dramatically, sometimes incrementally… Barbara Bell (www.captainbarbarabell.com), author of Flight Lessons: Navigating Through Life's Turbulence and Learning to Fly High, was one of the first women to graduate from the U.S. Naval Academy and the U.S. Naval Test Pilot School. Now she works to empower the next generation of female leaders. In 1992, Bell and fellow aviators went to Capitol Hill to help successfully repeal the combat exclusions laws, opening up combat aircraft and ships to women in the military. Bell holds a B.S. in systems engineering from the United States Naval Academy, an M.S. in astronautical engineering from the **Naval Postgraduate School**, an M.A. in theology from Marylhurst University, and a doctorate in education from Vanderbilt University.

UPCOMING NEWS & EVENTS:

Mar 7-9: Center for Executive Education LCSS Workshop
Mar 14: NWSI Seapower Conversation: Fighting the Fleet: Operational Art and Modern Fleet Combat
Mar 14-18: Center for Executive Education LCA Course
Mar 21-24: NWSI Nimitz Research Group Warfare Innovation Workshop
Mar 25: Winter Quarter Graduation

RESEARCH:

The Navy's New Mine-Hunting Systems Are Major Breakthroughs

(National Interest 24 Feb 22) … Kris Osborn

The U.S. Navy is making fast progress with new countermine technologies to track, identify, and destroy enemy mines.

Current efforts include the integration of the AQS-20C towed sonar system with the Barracuda mine-hunter drone. These advanced systems will be supported by manned and unmanned vessels.

Progress in testing, integration, and production has revealed new breakthroughs in technology that is capable of autonomously identifying and destroying mines. While countermine technology is nothing new, current developments indicate that the Navy has achieved long-standing goals in the realm of countermine warfare.

Leading Navy thinkers have been well aware of the threat posed by mines for years, and many have come to believe that mine-hunting capabilities will only become more important. A 2017 report from the **Naval Postgraduate School** identifies five key areas that the Navy must focus on in order to stay in front of the growing mine threat. Interestingly, the areas identified in the essay align very closely with the recent efforts of the Navy and Raytheon. The capabilities that the report identifies as most important "sensor range and resolution, automatic target recognition, and acoustic communications bandwidth" are entirely consistent with the aims of the AQS-20 and Barracuda programs.

In addition, the study specifically anticipates that "improvements to sensor range and resolution can be achieved by utilizing synthetic aperture sonar." Sure enough, that is exactly what the AQS-20 does. The overlap between the report and the AQS-20 system demonstrates how research on anticipated threats informs the Navy's innovations. Industry partners often invest internal funds in efforts to align with or anticipate what the Navy will need to address emerging threats.

By highlighting the need to reduce the "detect-to-engage" timeline, the report anticipated the recent effort to significantly reduce the sensor-to-shooter time of mine-hunting systems. Notably, this is what the networked Barracuda and AQS-20 systems are specifically engineered to do.

The Navy's New Mine-Hunting Systems Are Major Breakthroughs | The National Interest

Return to Index

No, There Is No 'Woke Military'

(Wonkette 25 Feb 22) … Robyn Pennacchia

Right now, as it concerns Putin's invasion of Ukraine, the American Right is in the "throwing shit up on the wall to see what sticks" phase. For the most part they've landed on a narrative involving Joe Biden cruelly ignoring Vladmir Putin's "legitimate security concerns" by forcing the sovereign nation of Ukraine to join NATO, even though Putin explicitly said he didn't want them to do that, basically forcing him to invade the country and maybe detonate some nuclear weapons on them.

But there is another they've taken a liking to, and which may be more likely to stick, given that the more one thinks about the "legitimate security concerns" narrative, the faster it falls apart — The Legend of the Woke Military.

This narrative, which dovetails with some other long-term goals involving getting to be shitty to other people without consequence, is that because of a couple army recruitment commercials focused on diversity (one imagines for the purpose of encouraging even more people to enlist), and also a TikTok video of a comedian pretending to be a White House intern that they've been obsessed with for the last year, Putin has decided that the American military is no longer super macho and therefore not a threat.

"How could Putin do this? Doesn't he know that western countries have the most diverse, equitable, and trans-inclusive militaries in the history of the world? And he's still messing with us? Wow," tweeted professional bigot Matt Walsh, as part of the usual 23 hours a day he spends Gargamel-ing about the existence of trans people.

Jake Bequette, a former Patriots tight-end and current Republican candidate for the US Senate in Arkansas, whined, "Our enemies see the pronouns-in-bio, 'diversity is our strength,' face-shield types leading our military," on Twitter. He added, "The U.S. never seeks war, but a good way to avoid it is to have Patton, Halsey, MacArthur, Grant, and Jackson types leading us."

Rudely, he did not add "That's what this country needs, more Nathan Hales!"

In a statement, QAnon heart throb Michael Flynn boldly suggested that all of the collective wokeness in all of the United States was perhaps to blame for Russia invading Ukraine:

Describing America as a systemically racist nation, the appointment of Marxists and other radical ideologues to positions of power, allowing millions to surge across our southern border, attempts to federalize and take over our election systems and processes, implementing racist CRT in our schools, our military and across our government, all along, raising the national debt closing in on $30 Trillion dollars, spending us toward extinction, all for left-wing causes.

There were also about 10,000 randos making super clever jokes about a they/them army, because of course there were.

Now, this all might then make one question why Putin would then have "legitimate security concerns" about Ukraine joining NATO, but that would require one being too smart to fall for this shit in the first place.

Since Bush II, at least, conservatives have been obsessed with the idea that only way to truly gain the world's respect and intimidate our enemies into behaving is by electing a raging buffoon with a serious toxic masculinity problem. While that has never actually worked out, per se, it has also never dissuaded them from getting their "No one's got a swell cleft in his chin like Gaston" on about it.

As a world class expert in machismo (see surname — some cultural stereotypes are real), I have some good news for these folks — our military is still a shining beacon of toxic masculinity. It is not now, nor has it ever been, "woke." The mere existence of our military, the amount we spend on it and what it does could not possibly be further from any semblance of "woke." Sure, they can put out ads recruiting diverse candidates, trying to push the idea that there is more to do in the military than help kill people; they can be minutely less shitty to transgender people and all women; they can even teach some enlightened courses at the military academy — all of that is absolutely nothing compared to some other shit. Particularly if we're talking about spending.

Machismo, by my own definition, is the spirit of doing incredibly pointless shit and having weird hang-ups because you think those things make you appear tougher and more manly, due to how incredibly insecure you are.

Thus, I can think of absolutely nothing more "macho" than the fact that the United States has spent $1.7 trillion on F-35 stealth planes that do not work — while millions of Americans across the country can't afford health care, can't afford child care, and nine million American children are living below the poverty line, 3.7 million of whom just dropped back there because the child tax credit expired. Because it was too expensive. Because starving children are not as important or as super cool as non-functioning stealth bombers.

In fact, you may recall that we could not manage to pass even the $1.7 trillion (over 10 years!) version of Build Back Better, despite the fact that studies showed it would actually result in a net profit by 2027. Because we need all of that money right the hell now for military stuff. Possibly for more nonfunctioning stealth planes.

Oh! Or so the military can pay $215,000 for 149 “non-vehicular clutch discs” that normally only cost $32 each. That is a $210,000 price difference. What's more macho than that? Oh, maybe the $84 million a year they spend a year on erectile dysfunction drugs? The $136 million they once spent sponsoring Dale Earnhardt Jr.? Or the other millions and millions they spent on NASCAR and other sports-related nonsense. A $100 billion bill for 600 nuclear missiles that experts say could "trigger an accidental nuclear war"? Oh, or just the $1 trillion we'll be spending on our nuclear force alone over the next three decades?

We spend more on our military than the next 11 countries combined — Russia only coming in third on that list. One reason we can do that is because unlike all of those other countries, including Russia, we don't have universal healthcare to pay for.

Perhaps if we really want to scare Putin, these are things we should advertise. Nothing says "fearless" quite like "We really don't care if any of our citizens live or die, we just want to win wars and have super big bombs and cool looking stealth planes that maybe don't work. And boners!" It's a little crazy, but it's the way we do things here, in America.

If that's not "not woke" enough for you, these macho, macho men can sleep better at night knowing that sexual assault is still a massive, massive problem in the armed forces. Nearly one in four servicewomen report having been sexually assaulted in the military. The GAO reports that women are 28 percent more likely to leave military service than are men, with most citing "family planning, lack of dependent care, sexism and sexual assault" as their reason for leaving.

And racism? Oh boy is there ever still racism. Just last year, a report on the Virginia Military Institute found widespread racism (and sexual assault) issues on campus, with one (white) cadet saying that he hears the "n-word" spoken by other white cadets “10 times a day from various people, that’s not an exaggeration.”

PBS reported last year that "numerous studies, including a report last year from the Government Accountability Office, show Black and Hispanic service members were disproportionately investigated and court-martialed. A recent **Naval Postgraduate School** study found that Black Marines were convicted and punished at courts-martial at a rate five times higher than other races across the Marine Corps."

Another report, this one conducted by Blue Star Families, found that 42 percent of service members of color had turned down assignments due to concerns about racism.

As for LGBTQ rights, sure — gay people and trans people are now allowed to serve openly in the military — but as of a 2020 study, 59 percent of LGBTQ servicemembers stay in the closet at work, for fear of repercussions.

Oh, and let's not even get started on the problem of white supremacist extremism in the military, what with many of our own homegrown terrorists joining up so they can learn how to kill us all better.

The entire purpose of the military is to kill people, usually poor people (on both sides), in unjust wars where we don't really know why we're there to begin with, but which apparently make very macho people feel super good. I don't think that's particularly "woke" either.

If not being "woke" is what makes a military intimidating, Putin must be terrified of us. Unless that's not actually a thing, as I suspect might be the case. It's almost as if none of this has anything to do with anything and all these people really want is to find a way to blame Joe Biden and a cultural zeitgeist they resent for the actions of a power-hungry dictator.

No, There Is No 'Woke Military' - Wonkette

Return to Index

FACULTY:

SWJ Book Review – Understanding Dark Networks: A Strategic Framework for the Use of Social Network Analysis

(Small Wars Journal 24 Feb 22) … Isaac Poritzky

Understanding Dark Networks provides an introduction to Social Network Analysis (SNA), a relatively new, and underutilized research technique that provides a view of dark networks unachievable in traditional lenses. SNA “can be used to gain a greater understanding of dark networks as well as craft strategies that undermine them”

The authors, Daniel Cunningham, Associate Faculty for Instruction at the Common Operational Research Environment (CORE) Lab embedded in the **Naval Postgraduate School**’s Department of Defense Analysis, Sean Everton, Professor in the Department of Defense Analysis and the Co-Director of the CORE Lab, and Philip Murphy, Associate Professor at Middlebury Institute of International Studies at Monterey are experienced scholars who have written extensively on “dark networks” and run the CORE

lab, whose mission it is to serve as the leading Department of Defense (DOD) organization in providing research and education to US and foreign military officers in advanced methodologies and cutting-edge, analytic technologies. SNA is the next essential methodology for DOD analysts, practitioners, and researchers.

Background on SNA

Valdis Krebs' (2002) seminal analysis of the 9/11 hijacker network along with Marc Sageman's (2004) study of 172 Islamic terrorist operatives, and many other studies, have laid the groundwork for the function and utility of SNA be it qualitative, quantitative, or mixed methods in security studies.

Critics of SNA argue that the three main challenges are "the dynamic and evolving nature of networks, the incompleteness of the data, and the fuzziness of boundaries". Cunningham, Everton, and Murphy argue that the main issue is not in finding dark network data, but sorting through it. Even with these challenges, SNA enhances our understanding of dark networks and potential strategies for disruption.

The majority of SNA research focuses on the usefulness for identifying key players whose removal from the network would disrupt it. That is one use, but Understanding Dark Networks raises the awareness of the wide range of metrics available and the various corresponding strategies. More so, it addresses how SNA can assist a myriad of kinetic (mainly targeting) and non-kinetic (tracking or monitoring, information operations, rehabilitate or reintegrate, and institution building) approaches to the tracking and disruption of dark networks.

Even in its simplest form, sociograms or visualized networks, SNA offers a powerful new perspective for those with an already solid foundation of a dark network. When more complicated quantitative analysis methods are undertaken—e.g., centralization and brokerage measures—SNA can explain a variety of behaviors due to its tendency to force researchers "to think in terms of constraints and options that are inherent in the way social relations are organized."

What truly separates SNA from other traditional quantitative approaches (i.e. frequentist statistics which focus on a random sample of actors and their attributes) is that SNA focuses on patterns that affect behavior. Concurrently, Cunningham mentions that analysts of dark networks often limit their focus to attributes, which can cause incorrect assumptions. An actor holding a mid-level position in a terrorist group is unlikely to gain significant attention due to their lack of formal prestige, but they may be a successful recruiter or key mentor for many lower-ranking members. SNA acts on the key concept that "actors do not make decisions autonomously; people are substantially influenced by the behavior and choices of other actors around them" . SNA allows researchers to transcend expected attributes and understand dark networks for what they really are: a group of complex social interactions and relationships that accounts for empirical context.

Structure of the Book

Understanding Dark Networks is split in four sections. The first section consists of three chapters that introduce readers to the assumptions, uses, collection, coding, and manipulation of social network data. Chapter 1 examines SNA and how it differs from other quantitative methods. It also exposes readers to basic SNA terms and concepts so that they will not become lost in later chapters.

The second section builds on the first section and explains the uses of several "families" of metrics commonly used for exploratory network analysis. Chapter 4 introduces readers to algorithms that identify a network's central actors. Chapter 5, positional analysis, introduces readers to algorithms that identify actors holding similar positions, e.g., the chief surgeons of different hospitals.

The third section consists of three chapters that focus on confirmatory techniques for examining dark networks. Chapter 9 focuses on hypothesis testing techniques for analyzing dark networks, mainly quadratic assignment procedure (QAP) and conditional uniform graphs (CUGs). Chapter 10 introduces exponential random graph models, which provide analysts with a way to examine the internal (endogenous) and external (exogenous) social processes. Chapter 11 examines methods for understanding changes in a dark network over time. The book concludes with a chapter that summarizes key items and lessons learned on which future research can build.

In general, Understanding Dark Networks functions as a textbook that provides basic explanations along with instructions on how to embark on several quantitative methods. Cunningham et al, focus on UCINET, but also address Net-Draw, Pajek, ORA, R, and Gephi. There is a significant lack of focus on Gephi, a popular software package, so this book would be most helpful for researchers interested in learning or growing their skills with UCINET. There are numerous images captured from these software packages that provide visuals to assist in understanding SNA. Along with the helpful images, the authors created tables that list the pros/cons, uses, interpretations, and potential caveats of different measurements. These tables are by far the most practical and useful addition to the book.

Understanding Dark Networks and SNA, in general, are an essential tool for the study of dark networks and criminal insurgency. Francisco Sollano (2022) conducted a SNA of Genaro García Luna, the former head of Mexican Federal law enforcement, and his ties to the Sinaloa Cartel [4]. This study helped to better understand the corrupt Mexican officials allowing illegal trafficking of drugs inside Mexico and into the United States. Sollano's which cited Cunningham et al and Everton's disrupting dark networks, study built on Jones et al's (2020) social network analysis of the Tijuana Cartel where he studied the "internal structures and the roles of individuals in cross-border polydrug networks under pressures from rivals and state leadership targeting" [5]. Dr. Jones was able to use SNA to understand the relationship between actor centrality and network topography, along with location of criminal activity, and location of residence. These studies are only the beginning of the usefulness of SNA.

Conclusion

Cunningham, Everton, and Murphy's book is most relevant for practitioners, researchers, or anyone seeking to understand dark networks. Practitioners often worry that SNA is difficult to learn and comprehend, but through Cunningham's easily accessible writing, anyone can understand and apply it after reading this book.Understanding Dark Networks would also have utility for teaching SNA to undergraduates, graduate, postgraduate students in many fields. The early chapters are accessible to anyone, but the last section requires baseline statistical knowledge.

Social Network Analysis represents the future of dark network analysis, ranging from jihadist groups to gangs. All intelligence analysts and researchers would see their research value increase with an in-depth understanding of SNA. Understanding Dark Networks: A Strategic Framework for the Use of Social Network Analysis should be an essential read for any practitioner or security scholar interested in learning or furthering their knowledge of SNA.

SWJ Book Review – Understanding Dark Networks: A Strategic Framework for the Use of Social Network Analysis | Small Wars Journal

Return to Index

New ACM TechBrief Spotlights Privacy, Ethics Problems with Facial Recognition Technology

(EurekAlert 24 Feb 22)

The Association for Computing Machinery's global Technology Policy Council (ACM TPC) today released "ACM TechBrief: Facial Recognition," a concise overview of an increasingly-used application which relies heavily on artificial intelligence. The brief includes a primer on facial recognition, key statistics about its growth and use, as well as important policy implications.

This latest edition highlights that the use of AI-driven facial recognition is "increasing despite its fundamental limitations, creating profound ethical and privacy concerns." The TechBrief's "By the Numbers" chart puts key statistics about its growth and use in high relief. For example, well over 80 million Americans (nearly 25% of the nation's population) now live in jurisdictions that have banned or heavily restricted the use of facial recognition systems largely due to privacy and civil liberties concerns.

A key concern outlined by the ACM TPC is that bias (including racial and gender bias) is both pervasive and profound in facial recognition systems. The TechBrief cites several research studies

demonstrating that errors often fall disproportionately on minority populations, particularly people of color.

"This is an urgent moment," explains Dr. Joshua A. Kroll, an Assistant Professor at the **Naval Postgraduate School** and lead author of the ACM TechBrief. "Articles about facial recognition have been all over the news lately and some of the world's leading companies are fundamentally rethinking whether or not to use the technology. But the public's understanding of the technology, as well as why it is controversial, is vague. The ACM Technology Policy Council developed this overview to familiarize people with the basics of facial recognition, as well as why many computing professionals are concerned about its potential negative impacts. We hope this TechBrief helps frame a public discussion of facial recognition and prevents people from being harmed by these technologies."

Another key concern raised in the TechBrief is the issue of privacy. The ACM TPC points out that anywhere there is a camera, individuals potentially may be identified and tracked. It therefore can be almost impossible to avoid this without avoiding public spaces. Moreover, many commercial systems are developed using facial recognition imagery gathered without the knowledge or consent of those depicted. In one recent example, the State of Texas announced that it is suing Meta for misusing facial recognition data.

"This new TechBrief complements a 2020 statement issued by the Association for Computing Machinery's US Technology Policy Committee (ACM USTPC), which urged an immediate suspension of the private and governmental use of facial recognition technologies," added James Hendler, Professor at Rensselaer Polytechnic Institute and Chair of the ACM TPC. "In theory, the deployment of facial recognition technologies could offer societal benefits. But, in practice, unregulated facial recognition use has the potential to cause harm to the fundamental human and legal rights of individuals in areas including privacy, employment, justice and personal liberty. We hope that by providing people with an accessible overview of facial recognition technology they will understand why it must be carefully regulated before it is even more widely adopted."

This TechBrief is the second in a series of short technical bulletins by ACM TPC that present scientifically-grounded perspectives on the impact of specific developments or applications of technology. Designed to complement ACM's activities in the policy arena, TechBriefs aim to inform policymakers and others about the nature and implications of information technologies. The first ACM TechBrief in the series focused on climate change. Topics under consideration for future issues include election security, smart cities, and encryption.

SWJ Book Review – Understanding Dark Networks: A Strategic Framework for the Use of Social Network Analysis | Small Wars Journal

Return to Index

How Much Damage Could a Russian Cyberattack do in the US?

(The Chron 25 Feb 22) … Scott Jasper, Naval Postgraduate School
(The Conversation 25 Feb 22) … Scott Jasper, Naval Postgraduate School
(Seattle PI 25 Feb 22) … Scott Jasper, Naval Postgraduate School
(Goskagit 25 Feb 22) … Scott Jasper, Naval Postgraduate School
(Malaysia Sun 25 Feb 22) … Scott Jasper, Naval Postgraduate School

U.S. intelligence analysts have determined that Moscow would consider a cyberattack against the U.S. as the Ukraine crisis grows.

As a scholar of Russian cyber operations, I know the Kremlin has the capacity to damage critical U.S. infrastructure systems.

Federal officials have been bracing for this. In January 2022 the U.S. Cybersecurity and Infrastructure Security Agency issued an alert that outlined the Russian cyberattack threat, with technical details of sophisticated Russian-led hacking from recent years. That included a complicated digital break-in that targeted the U.S. energy industry and gained access to the control rooms of U.S. electric utilities.

According to Homeland Security officials, the hackers "could have thrown switches" and knocked out power to the public – but did not.

In mid-February 2022, federal cybersecurity experts met with executives from big U.S. banks to discuss defenses against Russian hacking attempts.

In Ukraine, the Russian offensive began Feb. 23, 2022, with cyberattacks aimed at overloading and shutting down bank and government websites. In addition there were reports of software capable of corrupting data having been secretly installed on hundreds of computers owned by large Ukrainian organizations in the financial, defense and information technology services industries.

That malicious software spilled outside Ukraine – it was found on computers in Lithuania and Latvia – which is reminiscent of the NotPetya attack. In 2017, a piece of malware that initially seemed to be ransomware was unleashed on Ukraine and spread widely, causing more than $10 billion in collateral damage to major international companies. The NotPetya attack was ultimately attributed to a Russian military unit.

U.S. officials have also highlighted that Russian cyberwarriors can gain access and remain undetected for long periods in key systems in the U.S.

Russian Foreign Intelligence Service hackers did this in 2020 when they gained access to SolarWinds software, used by many companies and government agencies to manage their computer networks. After initially breaking into the system, the Russians stayed undetected for seven months, even disabling antivirus software and using stolen login credentials to appear like legitimate users.

This attack gave Russians access inside at least nine U.S. federal agencies and around 100 private companies, many in information technology and cybersecurity.

It's impossible to be certain there aren't more Russian government hackers lurking undetected in critical companies and systems in the U.S. And wherever they are, they may have the ability to cause substantial damage.

How much damage could a Russian cyberattack do in the US? (chron.com)
How much damage could a Russian cyberattack do in the US? (theconversation.com)
How much damage could a Russian cyberattack do in the US? | Conversation | goskagit.com
How much damage could a Russian cyberattack do in the US? (seattlepi.com)
How much damage could a Russian cyberattack do in the US? (malaysiasun.com)

Return to Index

Russia, China, and Iran: The Face of Competition in the Middle East

(MWI 25 Feb 22) … Kyle Atwell and Andrew Milburn

Russia, China, and Iran have all been learning how to conduct irregular warfare from the United States. They model their current irregular warfare approaches based on perceived lessons from observing US interventions in the world over the past few decades, according to arguments put forth in Episode 47 of the Irregular Warfare Podcast.

The episode examines strategic competition with Russia, China, and Iran—with specific focus on how this competition plays out in the Middle East. Our guests discuss how these states have used irregular warfare to achieve a position of geopolitical advantage over the United States. They go on to propose a solution, one that requires the United States to employ irregular warfare as part of an integrated strategy of deterrence. In order to do this successfully, the United States will have to look beyond platforms and invest in education, talent management, and human capital.

Dr. Seth Jones is senior vice president at the Center for Strategic and International Studies in Washington, DC. He also teaches at Johns Hopkins University and at the US **Naval Postgraduate School**. He is the author of multiple books, to include Three Dangerous Men: Russia, Iran, China and the Rise of Irregular Warfare—which serves as the basis for this conversation.

Rear Admiral Mitch Bradley is a US Navy SEAL officer and current commander of US Special Operations Command Central. He began his career as a SEAL in 1992, and has commanded at all levels

of special operations including as commander of the Naval Special Warfare Development Group. He is a graduate of the Naval Academy and holds a master's degree in physics from the **Naval Postgraduate School**.

The hosts for this episode are Kyle Atwell and Andy Milburn. Please contact them with any questions about the episode or the Irregular Warfare Podcast.

The Irregular Warfare Podcast is a product of the Irregular Warfare Initiative, a collaboration between the Modern War Institute at West Point and Princeton University's Empirical Studies of Conflict Project—dedicated to bridging the gap between scholars and practitioners to support the community of irregular warfare professionals.

Russia, China, and Iran: The Face of Competition in the Middle East - Modern War Institute (usma.edu)

Return to Index

Putin Just Pushed the World Into an Even Bigger Energy Crisis

(Foreign Policy 28 Feb 22) … Brenda Shaffer, Naval Postgraduate School

Even without sanctions, Russia's war will increase the shortage of oil and gas.

As we approach the 50th anniversary of the 1973 global oil crisis, international energy markets and the global economy are about to receive a similar jolt. Since Russia attacked Ukraine on Feb. 24, the price for crude oil has twice soared as high as $105 a barrel—a level last seen in 2014. And things could get a lot worse from here. Even if the current sanctions imposed on Russia do not explicitly target the energy trade, sanctions on banks and other entities will impede Russia's oil, natural gas, and coal exports, wreaking havoc on global energy markets. In addition, the dangers for oil tankers traveling in the Black Sea will reduce oil reaching global markets, including seaborne supplies from non-Russian producers such as Kazakhstan. The cut in Russian oil and natural gas supplies to markets will have spillover effects and further jack up the prices of coal and liquefied natural gas (LNG), adding another burst to inflation.

The crisis underlines that it's time for Western governments to be honest with their publics about the basic facts of energy security, restore their own energy production, and enhance the reliability of European energy imports. Even if the crisis with Russia is resolved soon—a very big if—Western governments need to make fundamental changes in their approaches to energy policy. The question of energy security was never gone, but Russia's war has put it back at the top of the agenda.

In coming days, Russian energy exports—oil, natural gas, and coal—will be significantly curtailed, even without sanctions. Traders buying energy cargoes, banks issuing letters of credit, shippers needing to insure their cargoes, and many other participants in the global energy trade will be cautious with all transactions and thus likely pass even on nonsanctioned ones involving Russia. This was the case with the recent round of sanctions on Iran. Companies tended to overcomply to avoid U.S. retribution. In the current case, companies will be even more averse to trading with Russia or processing Russian payments for fear of reputational damage and pressure from investors.

Just like the 1973 oil crisis, the current energy crisis is taking place while energy markets are already stretched. The tight market will amplify the impact of the lost Russian supplies. And unfortunately, all the signs are pointing to higher prices—perhaps much higher prices—that will be stay us even if the war comes to a quick conclusion one way or another.

Some politicians have been shocked by Russia's war into rediscovering the concept of energy security.

Prior to the current crisis, oil prices were high and on an upward trend. This was mainly because U.S. oil production plummeted at the start of the COVID-19 pandemic and has returned nowhere near pre-pandemic levels. All other major producers have been pumping at pre-pandemic rates, and there is very little spare capacity left in the global oil markets that could quickly come online to replace the shortfall in U.S. production or Russian exports. Global inventories of stored oil are also being rapidly drawn down, and there hasn't been enough investment in new production. Even OPEC has fallen substantially short of

its output targets, suggesting capacity is limited as existing wells decline and aren't replaced with new discoveries.

On the demand side, global oil consumption has returned to pre-pandemic rates—and is likely to continue to rise, especially once international travel snaps back. The pandemic led to higher base demand for oil: There has been increased use of plastics (which are made from petroleum) because of the rising use of masks, disposable goods, and various consumer wares as spending shifted online; at the same time, use of public transportation is sharply down as many people switched to cars.

Meeting this new oil demand without a further jump in price requires producing additional oil, something few Western governments have been willing to openly admit. And one of the only countries that has major underutilized oil production capacity is the United States. U.S. President Joe Biden's policies and his political base's sentiments against fossil fuels are major factors that have prevented fresh investment in U.S. oil production. Canada is another major global producer with substantial additional capacity, but it is constrained by transport, especially since Washington has been squeamish about the pipeline projects that would bring more Canadian oil to market.

This past weekend's new sanctions, though they were carefully constructed to exempt Russian natural gas exports to Europe, will inadvertently reduce them. Like the global oil market, the European gas market was already in crisis before Russia's invasion of Ukraine because of the European Union's own actions. In the hope of fostering greater use of renewable energy, the EU and individual European governments in recent years undertook policies that greatly hurt Europe's energy security, not least by putting the brakes on efforts to diversify energy supplies. While Europe has secured some new gas supplies, for instance by building LNG terminals and the completion in 2020 of the Southern Gas Corridor, which supplies Southeastern Europe and Italy from Azerbaijan, these projects have been nowhere near enough.

Brussels went further in hurting its ability to tap new gas supplies by ending most long-term natural gas contracts; one of the reasons was to force utilities to use more renewables. The long-term gas contracts had provided European consumers with secure supply at a stable price. Markets in Europe that have access to gas via long-term contracts, such as Italy and Greece, are faring much better in the current energy crisis than those that chose to rely on the spot market for gas. Ending long-term contracts and increasing gas trade at spot hubs strengthened Russia's ability to influence prices as the main swing producer with the ability to rev up and reduce supplies at the hubs. In recent years, European governments have also thoughtlessly reduced the scale of required gas storage, further hurting the continent's energy security. All this has been obvious to energy experts for some time.

Some politicians have been shocked by Russia's war into rediscovering the concept of energy security.

On Sunday, German Chancellor Olaf Scholz announced that Germany would begin to diversify its gas imports with the construction of two LNG import terminals, the country's first. Gas storage requirements will also be increased, and the Ministry for Economic Affairs and Climate Action is considering slowing down Germany's nuclear phaseout.

But the country with the largest potential for mitigating the energy crisis with new oil and gas supplies shows no sign of learning from the crisis. When White House spokesperson Jen Psaki was asked about the impact of the Ukraine crisis on the oil price on Saturday, she reiterated that the Biden administration will continue to concentrate on renewable energy. There was no sign of a shift to encouraging U.S. oil and gas production, let alone an increase in pipeline capacity to access Canadian supplies.

As it seeks to reduce energy inflation in advance of the U.S. midterm elections, the Biden administration appears to believe it has an ace up its sleeve: a renewed nuclear deal with Iran. Some believe that a deal will quickly bring additional Iranian barrels to market, leading prices to plummet again. This is unlikely to be much more than a temporary blip. Energy traders have largely factored in the expectation of increased Iranian supplies. And there may not be as much Iranian oil ready to ship as the administration believes. It's an open secret that a lot of Iranian oil is already traded. China already buys Iranian oil uninhibited. Iranian oil has many ways to circumvent U.S. sanctions—some is exported via Iraq and Kuwait, and there is a vast fleet of off-the-books oil tankers specializing in shipping Iranian

crude and other liquid fuels. Similarly, reports that the International Energy Agency is coordinating a release of strategic petroleum reserves by member countries, including the United States, don't signal much relief. Any price drop would likely be short-lived given the growing gap between production capacity and demand.

All this means that the United States and Europe won't be able to reduce prices unless they fundamentally reassess their energy security policies. Both U.S. and EU policymakers need to be frank with their publics and communicate that renewable energy sources—even if their buildout is accelerated—can't substitute for fossil fuels at anywhere near the speed required to make up for the shortage in oil and gas supply. What's more, weather-dependent wind and solar power require other energy sources—natural gas and nuclear power—to deliver a steady supply of electricity to homes and businesses. By promulgating the fiction that fossil fuels can be easily phased out and investments in maintaining production aren't needed, the United States and Europe have handed Russian President Vladimir Putin significant leverage over their energy prices. High energy prices can easily trigger a global recession, significant inflation, and massive popular discontent, as the world saw in 1973 and at other times since. It bears repeating: Like it or not, fossil fuels are in just about everything we do, including food that needs energy-intensive fertilizer to grow, tractors and combines to harvest, and trucks to bring to stores. Already, some factories have shut down or reduced production in Europe and China due to high natural gas prices, potentially sparking a recession.

Moreover, Europe should commission new pipelines for natural gas imports, including from the Caspian Sea region, the Eastern Mediterranean, and North Africa. The EU should end its opposition to European gas providers signing long-term supply contracts and mandate much higher gas storage to reduce the chance of shortages and maintain stable prices.

Energy security has always been a key pillar of national security. It's time for U.S. and European policymakers to recognize this basic fact and act accordingly—or they and their publics will face a very rough time in a worsening energy crisis.

Putin's War Set Off an Even Bigger Oil and Gas Crisis (foreignpolicy.com)

Return to Index

What the Trump Administration Brought to the Foreign-Policy Table

(Real Clear Policy 24 Feb 22) … S. Paul Kapur, Naval Postgraduate School

Critics have characterized the Trump administration's foreign policy as chaotic and unsystematic, but it was rooted in three principles that differed from both typical Democratic and Republican positions. Although the administration did not always articulate these principles, by bringing them the Trump team left a lasting impact on U.S. foreign policy that extends even to Trump's political opponents.

First, United States foreign policy must be simultaneously energetic and modest. The U.S. must actively pursue its core interests – the promotion of its security and prosperity – and respond decisively to threats against them. This response can range from forceful retaliation against provocations from individuals, groups, or countries to a general commitment to long-term strategic competition with adversary states. The United States' broader ability to shape the world is limited, however. Despite the nation's dedication to universal principles of freedom and democracy, the United States cannot ensure that human rights, competitive elections, or good governance take root overseas. Local histories, cultures, and political environments, as well as limited U.S. resources, will often make this impossible. Recognizing these constraints, the United States must resist the temptation to intervene abroad for reasons unconnected to its core interests.

Second, international institutions are not ends in themselves. Participation in them must clearly advance the United States' core interests in security and prosperity. Consequently, alliances, arms-control agreements, counter-terrorism partnerships, trade relationships and other cooperative arrangements require scrutiny, regardless of their history or their popularity with the expert class and the international community. Where they fail to advance U.S. interests because of free riding or other forms of cheating,

inequitable burden-sharing arrangements, or opposing national goals, they should be revised or abandoned.

Third, free trade, though desirable, is not a panacea. It can cause large swaths of the U.S. population to fall behind as traditional sectors of the economy wither. It can render the U.S. dependent on other states for access to critical goods and resources. And it can strengthen adversaries, enhancing their ability to compete with the United States economically, to threaten the security of the U.S. and its partners, and to challenge the rules that undergird the international order. The U.S. should promote free trade, but it must do so in ways that protect vulnerable segments of its own population and confront emboldened competitors who use newfound prosperity for disruptive ends.

These three principles do not mandate particular policies. But they provide a foundation for distinctive measures, as was evident from several Trump-era initiatives. For example, concern for the limits of U.S. power underlay the administration's decision to withdraw from Afghanistan after a 20-year intervention. A desire to address free trade's downsides impelled the administration to confront China over problematic trade practices, and to withdraw from what it saw as disadvantageous agreements like the Trans-Pacific Partnership. An insistence that cooperative institutions should clearly advance U.S. national interests led the administration to pressure allies to contribute more to collective defense, to withdraw from the U.S.-Iran nuclear deal, and to distance the United States from its longstanding counterterrorism partnership with Pakistan. And a willingness to defend core U.S. interests led it to wage an intense military campaign against the Islamic State, to kill terrorist masterminds such as Qasem Soleimani, and to prioritize competition with China and Russia as great-power rivals.

One need not support President Trump, or even agree with these foreign-policy principles, to recognize their importance. In fact, the Biden Administration, which claims to reject the Trump administration's foreign policy wholesale, has hewn to these principles to a considerable degree. For example, the Biden administration has declined to rejoin the Trans-Pacific Partnership. It has maintained Trump-era tariffs against China. It has followed through on withdrawal from Afghanistan, despite badly botching the process. It has largely ignored Pakistan. And it has remained committed, at least in principle, to prioritizing great-power competition with China and Russia.

Mr. Trump's political future is far from certain. But his administration's impact on U.S. foreign policy is not. The Trump administration brought to the table three principles to enhance America's ability to provide for its security and promote its prosperity. Future administrations, regardless of their politics, will have to contend with them.

S. Paul Kapur is a Professor at the **Naval Postgraduate School** and a visiting fellow at the Hoover Institution. From 2020-2021, he served on the State Department's Policy Planning Staff. The views in this article are his alone.

Putin's War Set Off an Even Bigger Oil and Gas Crisis (foreignpolicy.com)

Return to Index

Russian Cyberattack Risk May Spur US Cybersecurity Investments

(SP Global 25 Feb 22) … David DiMolfetta

The U.S. is preparing for Russian cyberattacks as the conflict between Russia and Ukraine escalates, a fact that may spur cybersecurity spending in the near term.

Tensions in Eastern Europe reached a boiling point this week after Russian President Vladimir Putin launched military operations in Ukraine on the evening of Feb. 23. U.S. President Joe Biden on Feb. 24 ordered sanctions to be levied on Russia's financial institutions, military and individual elites, following related moves from the United Kingdom and European Union.

Those sanctions could prompt Russia to respond with cyberattacks on U.S. financial entities and infrastructure, national security experts said, and analysts say the threat of such attacks will drive further investments in the security landscape.

"There is a growing concern that massive cyber warfare could be on the near-term horizon, which would certainly catalyze an increase in spending around preventing sophisticated Russian-based cyber attacks going after datacenters, networks, vulnerability points, and other highly sensitive data," Wedbush analyst Dan Ives, who focuses on tech stocks, wrote in a Feb. 24 research note.

Greater investment

The growing threat of Russian cyber action has underscored the need for organizations to bolster their security investments, Scott Kessler — global sector lead for technology, media and telecommunications at investment research company Third Bridge — said in an interview.

Kessler pointed to statistics from Microsoft Corp.'s October 2021 digital defense report, indicating that 58% of nation-state cyberattacks observed by Microsoft in that past year came from Russia and that such attacks have become increasingly more effective.

"I think that people need to be prepared for not just physical attacks with conventional weapons, but also cyberattacks as part of that process," said Kessler.

Sales in security products have been traditionally driven by the presence of cyberthreats, said 451 Research analyst Eric Hanselman. And he expects that trend to hold true amid the current conflict.

"It's a situation where prices tend to motivate action in buying and cybersecurity. And it seems a reasonable case to make that that's what we'll be looking at as there's heightened awareness," Hanselman said. The cyberwar environment gives security companies a strong incentive to innovate and sell more enterprise-level products, he added.

Ives said the companies most likely to see higher sales in the near term are Palo Alto Networks Inc., Zscaler, Inc., CrowdStrike Holdings Inc., Tenable Holdings Inc., Varonis Systems Inc., Fortinet Inc., Telos Corp., Mandiant Inc. and CyberArk Software Ltd.

"With many high profile cyber security attacks coming from Russia over the past few years, it's a matter of when not if this increased cyber warfare activity kicks into the next gear," the Wedbush analyst said.

Likelihood of attack

Some national security experts agree Russian cyberattacks on U.S. infrastructure are likely.

"If this crisis plays out, there is a not just a high likelihood, but a certainty of greater cyber activity, including targeting private sector actors," P.W. Singer, a senior fellow at New America specializing in 21st century warfare, said in an interview.

The degree and direction to which the attacks play out, however, remains to be seen, he added, noting that the attacks may fall on either financial sectors or supply chains.

Others in the space note that the Russian government takes a calculated approach to cyber warfare.

Despite all its actions against Ukraine, Russia may not have an incentive to intensify attacks against U.S. cybersecurity targets right now, said James Lewis, senior vice president and director of the Center for Strategic and International Studies' strategic technologies program.

Russia has been careful to avoid anything against the U.S. that would qualify as use of force, namely the destruction of critical services or an event that would lead to civilian casualties, Lewis added. It means that, regardless of the intensity of U.S. sanctions, Russia might not want to take any unnecessary risks.

"They'll not do anything that makes it harder for them to manage what they gain in Ukraine," Lewis told Market Intelligence.

But with so much uncertainty around Russian thinking and plans, governmental organizations and private companies alike have to be prepared for unpredictable situations. Robert Lee, founder and CEO of Dragos Inc., said that these are moments when "low probability high consequence" attacks turn into "unknown probability" scenarios.

"We are in uncharted territory and we know that some states, especially Russia, leverage cyber operations in such times as a military and political tool that crosses the bounds of what our imaginations would hope are red lines," Lee said in an email to Market Intelligence.

Preparations underway

The Cybersecurity & Infrastructure Security Agency last week issued a "Shields Up" alert in response to the growing Russian threat, indicating that "every organization in the United States is at risk from cyber threats that can disrupt essential services and potentially result in impacts to public safety."

The alert said organizations should be ready to detect unusual network behavior, as well as make sure all software is up-to-date and that all remote access requests are validated with multi-factor authentication, among other things.

Even if Russia does not directly attack large, global companies, there is potential for collateral damage against U.S. organizations that operate in Ukraine, do business with Ukrainian companies or have supply chain presence in Ukraine, Adam Meyers, senior vice president of intelligence at cloud security titan CrowdStrike, said in an email to Market Intelligence.

Meyers encouraged organizations to prepare and adopt a heightened security posture. "As the impact and reactions to the announced sanctions begin to take hold, the intentions of Russian threat actors may shift," he said.

One possible solution would be for companies to implement extended detection and response, or XDR technologies, into their security frameworks in order to protect against threat actors, said Scott Jasper, a senior lecturer at the **Naval Postgraduate School** in Monterey, Calif., and author of Russian Cyber Operations: Coding the Boundaries of Conflict.

XDR, which integrates multiple security protocols under one roof, would allow organizations to check for anomalistic behavior inside a secure network, Jasper said. He cited Russia's 2018 attack on the U.S. power grid, which was achieved with no malware, but instead with just compromised credentials.

The president in a Feb. 24 press conference reaffirmed the U.S.'s readiness stance against Russian cyber operations.

"If Russia pursues cyberattacks against our companies or critical infrastructure, we are prepared to respond," Biden said. "For months we've been working closely with the private sector to harden our cyber defenses and sharpen our ability to respond to Russian cyberattacks as well."

Market movement

Broader markets responded unfavorably to Russia's offensive, with multiple broader indices initially diving into correction territory Feb. 23 before recovering some losses following the announcement of new sanctions. The S&P 500 closed Feb. 24 down 1.4% for the week-to-date, while the Dow Jones Industrial Average closed down 2.5% for the same period.

Russian cyberattack risk may spur US cybersecurity investments | S&P Global Market Intelligence (spglobal.com)

Return to Index

ALUMNI:

SPOC Names Timothy R. Jett as Chief Operating Officer

(Trussville Tribune 25 Feb 22)

SPOC welcomes Timothy (Tim) R. Jett as the new Chief Operating Officer (COO).

Jett has over 30 years of progressive leadership experience and was most recently a Technical Program Manager with Amazon Web Services. Prior to his work with Amazon, Jett had a long and highly successful supply chain career in the U.S. Navy; he brings unrivaled logistical experience to SPOC. As commanding officer in the U.S. Navy Fleet Logistics Center, Jett led a team of over 400 military and civilian personnel and oversaw billions of dollars of material and equipment. He is certified Level III Life Cycle Logistics through the Defense Acquisition University and Defense Acquisition Workforce Improvement Act (DAWIA).

"We are excited to bring Tim on board as SPOC continues a trajectory of growth and expansion," CEO of SPOC, Robert L. Mason, said. "His seasoned leadership and experience will aid in our mission to further sustain initiatives both internally at SPOC and helping others reach their ESG and operational goals."

Jett graduated from the United States Naval Academy, earning his Bachelor's degree in economics; he also holds an MBA in logistics and supply chain management from the **Naval Postgraduate School**. His move back to Alabama is a homecoming of sorts; he grew up in Scottsboro, about two hours northeast of SPOC headquarters.

When he's not working, Jett and his family spend time together exploring this area and finding the best places to eat. An avid road and mountain cyclist, he's also ready to hit the trails and discover the area's most exciting places to ride.

In early 2021, the company announced the successful deployment of 70,000 inverters into the harshest industrial environments, producing an annualized energy savings of more than half a billion dollars and reducing C02 emissions by over 3.6 million metric tons per year. As SPOC grows, so has the executive team.

Jett's role will be pivotal in the company's growth, as he oversees the day-to-day operational functions of SPOC and its family of companies. His role is to provide leadership while effectively communicating and fostering growth among the family of SPOC companies and all team members.

SPOC names Timothy R. Jett as Chief Operating Officer | The Trussville Tribune

Return to Index

Compton, Winn to Receive Scouting Award

(The West Alabama Watchman 25 Feb 22)

Rear Adm. Bryan Whitfield Compton Jr. of Demopolis and Luther Winn Jr. of Eutaw are the recipients of the 2022 Hugh A. Lloyd Lifetime Scouting Achievement Award.

The two will be honored by the Black Warrior Council Boy Scouts of American at a luncheon Thursday, March 10, at Soggy Bottom Lodge's Shack 33 in Linden.

In addition to honoring the two men, the Council will be celebrating 100 years of service to West Central Alabama. Those attending the luncheon also are given the opportunity to use Soggy Bottom's sporting clay course for $100 per shooter.

Rear Adm. Bryan W. Compton Jr.

From 1951 to 1982, Compton served in the Navy. During his time of service, he commanded thousands of men and flew more than 5,500 flight hours with 1,116 carrier landings. His service did not go unnoticed as he is the holder of the Navy Cross, six Distinguished Flying Crosses, the Bronze Star Medal, 19 Air Medals, three Navy Unit Commendations and one Navy Commendation Medal.

A graduate of the U.S. Naval Academy, Compton earned his wings in May 1953. He served numerous missions and commands, including two combat tours of Vietnam. After being sent to the U.S.S. Enterprise, the first nuclear-powered carrier, he was sent to War College and nuclear power school. He then became the first commander of the super-carrier U.S.S. Nimitz. Compton achieved the rank of admiral in 1976.

The admiral has an Associate of Science Degree from Marion Military Institute, a B.S. from the U.S. Naval Academy and an M.S. in Electrical Engineering from the U.S. **Naval Postgraduate School**.

Born in San Angelo, Texas, Compton spent most of his civilian life in Demopolis with his grandfather. He is married to the former Maxine Anderson. They have four children, Bryan W. III, Mary, David, and Eleanor.

Luther Winn Jr.

Since 1999 Winn has been the president and CEO of Greenetrack, Inc., the largest African American owned gaming facility in the United States. He brought with him more than 20 years of experience and leadership in the gaming industry and has received numerous awards reflecting his commitment to his community.

Greene County, home to Greenetrack, was singled out in 2008 by the Alabama Bureau of Analysis as the fastest growing county in Alabama. The county was once listed as the poorest in the state. Under Winn's leadership, Greenetrack and the implementation of gaming saved Greene County, creating four hundred jobs in 2004.

From 1992-1999, Winn served as Director of Racing at Gulf Greyhound Park in LaMarque, Texas. He was the first African American Director of Racing in the United States, he worked closely with the owner to open the facility, and he assisted with the implementation of policies and procedures to ensure best practices.

He also assisted in the opening of gaming facilities in Coeur d'Alene, Idaho and in Council Bluff, Iowa.

Winn began his career as a security guard and paddock judge for the Greene County Greyhound Park in 1978. In 1988, he was promoted to overseeing the racing department.

Winn attended Alabama A&M University in Normal. A supporter of the BSA and the American Cancer Society, he also sits on the boards of the Greene County Industrial Development Authority, West Alabama Mental Health and the National Action Network. He is a co-founder, sponsor and mentor of My Brother's Keeper Boys' Academy, an organization geared towards uplifting the youth of Greene County.

Compton, Winn to receive Scouting Award – THE WEST ALABAMA WATCHMAN

Return to Index

How To Build Leadership Programs For Women In Your Organization

(Global Trade Mag 25 Feb 22) … Barbara Bell

The percentage of women who hold leadership roles in business, higher education and government grows with each passing year – sometimes dramatically, sometimes incrementally.

But every gain holds the promise of more gains, as young girls see opportunities previous generations didn't.

"Each of us stands on the shoulders of all the women in our chosen professions who have come before us, who have blazed a trail," says Barbara Bell (www.captainbarbarabell.com), a professor of leadership at Vanderbilt University and author of Flight Lessons: Navigating Through Life's Turbulence and Learning to Fly High.

"Others have done the hard work, and we must too. Throughout my career, I learned many deepening skills of leadership and was privileged with many opportunities to lead."

But Bell, one of the first women to graduate from the U.S. Naval Academy and the Naval Test Pilot School, also says that businesses and other organizations can do a much better job of helping women reach their leadership potential. And March, which is Women's History Month, is as good a time as any to get started.

She says some ways organizations can develop better leadership programs for women include:

Provide mentors or a support system. Certainly, a mentor can guide and advise those emerging leaders in an organization, which is valuable in and of itself, Bell says. "But it goes beyond just having someone who offers guidance," she says. "It's important as women are developing their leadership skills to have someone in their corner." Bell says that when she was an instructor at Navy Test Pilot School, she worked for a Navy department head, Commander Dave Kennedy, and a Marine Corps Commanding Officer, Lt. Col. Bob Price, who did that for her. "Both of these leaders supported my work and, more broadly, helped expand the roles of women in military aviation," she says.

Allow them time to grow. Bell says that, too often, people think they need to have everything figured out before they take the risk of heading down a new path or beginning a new opportunity. But organizations can help women grow as leaders if they free them of this idea. “Women need to understand that, as you become more senior in your leadership, you should let go of the notion that you have to know everything,” she says. “They also should understand that as their leadership responsibilities grow and become increasingly more complex, they should become comfortable being more of a generalist. One way of growing in leadership is to rely on those who work for you as the specialists and lead them in the direction you want them to go.”

Encourage, don’t discourage. It’s easy to point out obstacles someone faces and to express doubts about their abilities to overcome those obstacles, Bell says. Avoid that temptation. She recalls a career manager in the Navy who suggested her record wasn’t strong enough to get into Test Pilot School. “Fortunately, I didn’t let him dissuade me,” she says. “By that point in my career, I was so used to the naysayers that I was not fazed.” But it did affect her approach when she became a career manager later herself. She vowed never to discourage, but only to encourage those she worked with.

Understand that women leaders can be role models for others in the organization. In flight school, Bell became a role model almost by default because she stood out as the only woman in her Naval Flight Officer class. “My calling to leadership included the privilege to be the example,” she says. “Other women who assume leadership roles have the same opportunity and privilege.” And having role models who inspire others is good for any organization.

“For anyone, rising to the top takes hard work, endurance and persistence,” Bell says. “You have to be in it for the long haul. But whenever we create forward motion in our lives, we generate the lift that will take us to new heights.”

Barbara Bell (www.captainbarbarabell.com), author of Flight Lessons: Navigating Through Life’s Turbulence and Learning to Fly High, was one of the first women to graduate from the U.S. Naval Academy and the U.S. Naval Test Pilot School. Now she works to empower the next generation of female leaders. In 1992, Bell and fellow aviators went to Capitol Hill to help successfully repeal the combat exclusions laws, opening up combat aircraft and ships to women in the military. Bell holds a B.S. in systems engineering from the United States Naval Academy, an M.S. in astronautical engineering from the **Naval Postgraduate School**, an M.A. in theology from Marylhurst University, and a doctorate in education from Vanderbilt University.

How To Build Leadership Programs For Women In Your Organization - Global Trade Magazine

Return to Index