IW Panel Questions and Answers – 5 May 2020

Due to time limitations and the tremendous interest in our recent Information Warfare Panel, the panel was unable to address all questions posed by attendees. Several panelists agreed to provide answers to questions after the fact. We share them below to foster a continued dialog on this important subject.

[*Max Thibodeaux*]: If a commercial activity was able to offer AI solutions such as deep fake video production to communicate in native languages, how could the commercial sector be assured that there is a market available in the national security area for this? What would be the entry point? Are efforts such as DIU and AFWERX the way forward for these kinds of offerings to focus and de-conflict them?

[*Matt Venhaus*]: I think that there will be a growing market for this kind of capability. Beyond DIU and AFWERX, I think that SOFWERX, and the USCYBERCOM-hosted DreamPort would be interested.

[*Paul Lieber*]: Sadly, the bigger DoD and sister agency tech discovery initiatives continue to fall woefully short at ID'ing and executing cutting edge tech. I would suggest commercial and national security sectors look for smaller wins and test cases to validate concepts. This also removes much of the bloat inherent. A key would be to isolate – and protect – commercial sector offerings to allow them to flourish.

[*Dean Worley*]: There is an incredible boom in all aspects of leveraging AI/ML in commercial sectors globally. The interesting thing is that many of the same technical approaches (e.g., generation of "Deep Fakes" and advanced course of action development) that can be used for national security requirements, also have very legitimate business applications in the entertainment, gaming, and even educational/teaching industries and systems. Besides DIU and AFWERX, other "entry points" include the Joint Artificial Intelligence Center (OSD's JAIC), SOFWERX, and the emerging academic and FFRDC/UARC ecosystem that's grown over the last decade.

[*JJ Johnson*]*:* @Brian Pierce, how does an organization or enterprise infuse a culture of cognitive resilience?

[*Brian M. Pierce*]: Cognitive resilience at the individual and organizational levels is improved through education that involves critical thinking. Three such efforts are as follows:

1) Finland has established a national education program that places the country as first in media literacy for Europe, where media literacy is indicative of cognitive resilience.
2) The "Bad News" online game developed by the Cambridge University researchers, Jon Roozenbeek and Sander van der Linden. In the game, players take on the role of a fake news producer to become better educated on the

strategies used in the production of fake news. Research has shown that this game experience strengthens critical thinking and media literacy.

3) The Civic Online Reasoning curriculum developed by Professor Sam Wineburg and colleagues at Stanford. This curriculum helps students improve their online media literacy through, for example, strategies to answer three questions that should always be asked when coming across unfamiliar online content: Who's behind the information? What's the evidence? What do other sources say?

Given the deluge of disinformation that can overwhelm us in today's hyperconnected world, technology can help enhance our cognitive resilience against this onslaught. This technology includes the automated detection of manipulations of multi-media, and other tools.

[*Kim Underwood*]: What can the U.S do in the near term (in 1-2 years) in the information war versus longer term goals?

[*Matt Venhaus*]: In the nearest term, unify authority and oversight both within and amongst the Federal Departments to provide meaningful, dedicated, full-time leadership to the Information Competition. For DoD specifically, fully embrace the NDAA Section 1631 dictate to assign a Principal Information Operations Advisor. Give this person the seniority and the staff necessary to fully oversee the entire enterprise.

[*Paul Lieber*]: Concur with above. In tandem, mandate inter-discipline and agency IW teams to regularly meet, coordinate and (from a StratComms-like model) orchestrate and organize effects. No need for another new or synchronizing body. Place a qualified (PhD, mass comm/assessment professional) in a Strat Comm position at each to keep his/her house in order.

[*Boots Winn*]: Do you see IW as a "convergence" or an "integration" activity? Is it analogous to combined arms integration or a transition to something different?

[*Matt Venhaus*]: I think that the technology converges, but the disciplines integrate. The advent of armed aircraft performing close air support was both a convergence of technology (flight with artillery), but the unique nature of CAS did not eliminate the need to integrate air and artillery operations to achieve maximum effect. Similarly in IW, while the transmission of electrons through the air or down a wire may seem to make us think that all of IW is converging on the cyber domain, in truth, we still need the unique expertise of those different disciplines who can deal with what comes out the other end. If what comes out the other side is machine readable and manipulates or replaces code, that understanding is fundamentally unlike similar electrons that produce a human readable message. Maintaining unique disciplines

for each type of employment allows for the specialization of our talent and prevents a "jack of all trades, master of none" approach to talent management.

[*Paul Lieber*]: Integrate. Each shape each other's environments. Way too much time is wasted on trying to define terms/converge disciplines. Doctrine and authorities always get in the way.

[*Sheila Boozell*]: According to Alliance for Securing Democracy, Russia is moving into a weaker power status. Yet the US persists on going on the defense rather than the offense when Russia goes on the offensive. Could panel members discuss why we continue to play a "defensive" game vice an "offensive" one? Is our hesitancy due to culture, political will, or the perception of US hegemony on the global stage?

[*Matt Venhaus*]: I think that culture and political will (derived from culture) each play a part. Our American values of free expression and independent media as a check on power make us reluctant to operate in the same ways as our adversaries currently do. This has led us to a hesitancy to act in all cases to avoid "becoming what we despise." What we as a Nation have failed to come to grips with is that we can stay true to our values AND operate aggressively. Censorship and control over the flow of information is the time-honored path of the tyrant. Breaking through those walls (with force and vigor), exposing people to new ideas from which they can make their own judgments, and allowing the marketplace of ideas to flourish has always been America's path. Our current competitors have a tremendous fear of losing control over the information that flows to their citizenry. We should help them see that fear come to fact. Defense of our own people's cognitive security and information resiliency will remain important (defense), but it will only be effective when combined with destructive penetration of foreign media space and forceable insertion of our ideas and our ideals.

[*Dean Worley*]: My only add to this: the adversary gets a vote. In this particular case, Russia's effective use of the information environment has also deterred the US and its Allies and partners in Europe from taking effective actions, especially during the 2008-2016 period.

[*Paul Lieber*]: We're decades behind in this space, partially due to authorities (requiring attribution). Also, questions of moral/ethical behavior norms inhibit the US' response (as adversaries aren't concerned). These are both wrong, as dis and misinformation are parts of any/every information environment. It's no different than partial or selective disclosure. We need to have the stomach for it.

[*Scott A*]: There is one rule: we have everything to lose and the adversaries have everything to gain. It's another disadvantage for us. What gloves to we need to remove to respond?

[*Matt Venhaus*]: See above.

[*Dean Worley*]: I see this in a different way. From a realist perspective, our most likely competitors and adversaries have a tremendous amount to lose, especially in paying the ultimate price in maintaining their power – and with that, their lives. That gives us leverage and is a natural arena for strategic-level integration of US instruments of power to allow us to achieve our national security policy goals. As far as loosing gloves, the 2018 publication of National Security Presidential Memorandum 13 (NSPM 13) was a significant loosening of the restrictions on cyberspace weapons development and employment.

[*Paul Lieber*]: Insert true scientists (not contracted rears in seats), supported by tools – into the equation. Almost every time I have this conversation, those I converse with wonder why they didn't hire someone 'like me.' Yet never attempted to hire and empower someone 'like me.'

[*Herminio Blas-Irizarry*]: Is our Government currently well organized to conduct synchronized IO to foreign audiences?

[*Matt Venhaus*]: No, but it is the Government that we have. Reorganization is a long-term proposition. Making the current instantiation of our system work more effectively is a better short-term strategy.

[*Paul Lieber*]: Organization is less important than mindset. Be ahead of the curve versus trying to organize curves. The cream will rise to the top, collectively. Those that don't…will become irrelevant.

[*Michael Stone*]: Where and how do you see the U.S. government improving the means and methods to develop and implement deliberate national strategy that combines actions across our own instruments of national power for synergistic influence effect? Our adversaries in the current competition do this with comparative ease. How does the U.S. compete above the current bureaucratic and cultural roadblocks for effective collaboration above the operational/tactical level?

[*Matt Venhaus*]: I think that the post-9/11 example of the creation of DHS and the National Counter Terrorism Center (NCTC) provide some useful, if incomplete examples. NCTC was envisioned as the ultimate Intel Fusion Center because the 9/11 report concluded

that there was enough information out there to have prevented the attack, but it wasn't being fully aggregated and wasn't getting into the right hands for action. In the information space, the problem is not so much a lack of intel fusion, but a lack of coherent direction coupled with the authority to direct. A National Information Competition Center could only be useful if empowered to direct the Departments and agencies to conduct activities within their capability areas according to a unified plan. Planning and authority must be consolidated.

[*Paul Lieber*]: They need to start with better problem ID and assessment…and work backwards from there. Current approaches intentionally silo, then write conflicting policy that formalizes this. Use education and training as a reinforcing conduit.

[*Erik Olsen*]: With the incredible amounts of reporting being produced on disinformation from across the WoG, what are your thoughts on FEMA standing up a disinformation Task Force as an effort to synchronize and aggregate these efforts?

[*Matt Venhaus*]: I think that empowering a domestic agency to handle protecting the Homeland from ill effects is the right idea. It should not be the DoD or IC who protects the domestic information environment. FEMA, with its focus on natural disasters, wouldn't be my first choice, but you are on the right track with making it part of a domestic agency (DHS, DoJ, DoC, etc.).

[*Paul Lieber*]: Concur; great idea. Definitely a new approach to an old problem. And re-scoping mis and disinformation as a security versus information/narrative threat will finally remove the cotton balls from individuals' ears.

[*Dean Worley*]: There might be another approach to consider: leverage the authorities and precedents of entities such as Joint Interagency Task Force-South (JIATF-South). See if a JIATF could be established with emphasis on protecting the Homeland in the information environment (perhaps JIATF-IE?).

Questions Answered During the Webinar

[*JJ Johnson*]: Recent reporting from the EU External Action Service indicates a convergence of disinformation themes among Russia, China and Iran, which have traditionally operated in accordance with their own national goals. What is your assessment of the impact of this trend, and how can we respond and adapt?

[*Matt Venhaus*]: I think that our adversaries are converging around similar opportunities, but that their national interests remain distinct. The themes chosen generate the immediate effect, which may be similar, but the long-term outcomes follow distinct separate paths. That said, the more powerful that the biggest actor appears, the more likely that alliances will form against that actor despite the resulting strange bedfellows. If everyone seems to be hating you, maybe it's you?

[*Brad Young*]: Thank you for hosting this panel. My name is Major Brad Young, grad student at the Naval Postgraduate School studying Information Strategy and Political Warfare. My question is Army-related, and for any of the panelists: "In your opinion, is the Army currently organized in a way to maximize the relationship between IO, cyberspace operations, and other IRCs? What can we do (training, organization, etc) to improve the operational effectiveness of our Army FA30 (IO Officer) community to conduct information warfare in current and future conflict?" Thank you again.

[*Nothing additional provided*]

[*Herminio Blas-Irizarry*]: Should the USG consider the re-establishment of the U.S. Information Agency to synchronize all USG messages?

[*Matt Venhaus*]: Not as it was originally constructed. USIA only partly centralized coordination and never coalesced funding or directive guidance. Standing up an organization that is fully empowered, funded, and staffed would be necessary.

[*Rick Lipsey*]: The nation is facing a growing struggle to conduct free and fair elections in the face of growing misinformation and disinformation. Do you have specific suggestions on how to combat this problem?

[*Matt Venhaus*]: The struggle is not to conduct elections; the struggle is for the confidence of the voters that the election is free and fair. To maintain/enhance that confidence, we must compete with our adversaries using both offense and defense. Offensively, we must threaten and/or act asymmetrically to reduce interference by foreign governments. The recent Russia/OPEC deal regarding oil supplies was much more important to the Putin regime than it was to OPEC. Had we sought to prevent or disrupt that deal unless/until the Russians showed a demonstrable reduction of bot activity on Facebook, we might have gotten their attention. Coupling that with defensive practices to secure voting systems, and voter rolls along with enabling easy identification of foreign-originated content could be effective.