Department of Political Science
University of Cincinnati
PO Box 210375
Cincinnati, Ohio 45221

Crosley Tower 1100
(513) 556-3314

Preliminary Written Responses
Cybersecurity Sub-Committee
United States Senate Armed Services Committee
Professor Richard J. Harknett, University of Cincinnati, USA
February 13, 2018

"Department of Defense's role in protecting democratic elections"

The Subcommittee is concerned that, in the lead-up to the 2018 and 2020 elections, the Department and government as a whole have not sufficiently deterred future interference, leaving our democratic institutions at risk to foreign intrusion.

The Subcommittee is correct in its concern. The likelihood of foreign intrusion (not just Russia, but other revisionist actors as well) is high due to the nature of this domain. Cyberspace is an interconnected domain and yet all our approaches rest on a principle of segmentation, instead of seeking synergies of expertise. Our adversaries have figured this out. Cyberspace is a new Seam in international power competition in which strategic effect can be produced below the threshold of war and the reach of traditional deterrence strategies. We should assume as a starting point that adversaries will engage in cyber operations against our national sources of power, including economic wealth and social-political cohesion. If we do not actively engage these strategic cyber campaigns, we will suffer. We need a new strategy that rests on a seamless operational environment of 1.) integrated resiliency, 2.) forward defense, 3.) contesting adversaries' capabilities and 4.) countering their campaigns. Through this new strategy, we can actively erode the confidence that our adversaries have in achieving their objectives and in their capabilities. Over time this may produce a deterrent effect, but that can only be achieved through persistent efforts to seize the cyber initiative away from our adversaries.[1]

In traditional great power politics, national sources of power were vulnerable only through direct violation of the territory upon which they centered. Thus, we came to equate strategic effects with war, and to narrow the central role of the state to promoting territoriality (its sovereign territorial integrity). The interconnected nature of cyberspace, however, means that now our national sources of power are vulnerable to manipulation without direct assault across territory. Strategic effects can occur without war through this new seam—and we should expect adversaries to explore it. We must contest this effort and seize back the initiative. In order for this to occur and positively affect the electoral cycle, we must position the Department to

[1] For more on persistence, see M. Fischerkeller and R. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* 63 1 (Summer 2017): 381-393.

contribute to the defense of electoral integrity, protecting the vote and the voter. Electoral integrity cannot be protected by leaving civilians alone on the front lines.

Are the roles and expectations of the Department clearly defined with respect to protecting U.S. elections process from foreign influence in the cyber domain?

They currently are not sufficiently defined nor enabled. Most importantly, we must move away from 1.) our "doctrine of restraint"[2] that forces us to defend in our own space after the first breach is detected, and 2.) away from the tendency to view every intrusion as a law enforcement problem first. Cyberspace is an interconnected domain of constant contact, which creates a structural imperative to persist. Persistence in resiliency, forward defense and countering is necessary because the analytical categories of offense and defense do not actually hold in this space—it is too fluid and dynamic. As former Deputy Director of the National Security Agency Chris Inglis put it: "It's almost impossible to achieve a static advantage in cyberspace – whether that's a competitive [offensive] advantage or a security [defensive] advantage – when things change every minute of every hour of every day. And it's not just the technology that changes; it's the employment of that technology; the operations and practices."[3]

Our protection posture must be moved as close to the sources of adversarial action and capability as possible so that we can watch, react, disable, and disrupt at a speed of relevance (defined as one step ahead of the adversary). We forward deploy in terrestrial space, where actual time and distance still matter for defense, so why do we hesitate to do so in the one domain where time and distance are crushed and cannot be leveraged for defense? Garrisoning our cyber forces has created a great disadvantage for us and invites opportunity for our adversaries. DoD is not on the front lines, which because of interconnectedness, are everywhere. We need to secure through a persistent pursuit of the initiative if we are to manage this new seam in international power competition.

How can the Department use its national mission teams' offensive capabilities to improve deterrence?

National Mission Teams (NMTs) can eventually produce a deterrence effect, but not by relying on deterrence strategy. Cyber strategic effects do not come from mere possession and the threat of employment, but from actual use. It is critical to differentiate between deterrence strategy and deterrence effects in answering this question because they get conflated too often. We can achieve a deterrent effect through other means than a deterrence strategy. Deterrence strategy rests on the prospective threat of punishment or denial to convince someone not to take an action. This dynamic cannot work in a strategic environment of constant action. Cyberspace is a strategic environment of initiative persistence (one can always find the willingness and capacity to get one step ahead). Our NMTs must be charged with eroding adversary confidence and deployed capability, not sit idle as prospective threats to impose costs in the face of cyber operations below the level of war. Cyberspace operations should be treated as a necessary national security activity and as a traditional military activity. Persistent erosion of confidence

[2] Department of Defence, *DOD Cyber Strategy* (2015).

[3] Chris Inglis as quoted in Amber Corrin, "Is government on the wrong road with cybersecurity?, *FCW: The Business of Federal Technology* (May 21, 2013, https://fcw.com/articles/2013/05/21/csis-cybersecurity.aspx.

and capability will shape adversaries' behavior, over time, toward more stable norms. If we make the strategic effects sought by adversaries inconsequential, their penchant for attack may diminish—then we may get a deterrent effect (i.e., adversaries may determine it is not worth it to confront us). But we will not get there without allowing our NMTs to hunt, disrupt, disable cyber activities, and thereby seize the initiative back from our adversaries. We must understand this cyber persistent space not as an unstable escalatory environment, but rather as a fluid environment in which the initiative is always in play and we must seek initiative control.

Is the Department's conception and implementation of deterrence sufficient?

The Department's Cold War conception of deterrence does not map to the realities of this new strategic environment. Deterrence is an approach to security, not the approach. We cannot rely on a strategy in which the measure of effectiveness is the absence of action if we hope to manage an environment of constant action. The cost-benefit calculus an adversary may hold within cyberspace is never stable enough for us to be certain that our static deterrent threats are credibly influencing adversaries. There are always new and cost-effective opportunities for them to explore. They can constantly manipulate the data, networks, tools, and vulnerabilities that are coming on-line daily thanks to the efforts of malware developers and the innovations of the market. The cyber terrain to secure and the means to traverse that terrain are always changing. There is too much incentive and potential for adversaries to refrain from persisting in cyber activities below the level of war.

In short, deterrence is a strategy reinforced by segmentation (borders/thresholds), sovereignty, relative certainty, and territoriality. Cyberspace by contrast is defined by none of those conditions; it is defined instead by its interconnectedness, constant contact, relative anonymity, and a lack of territoriality. Just as nuclear weapons precluded defense and necessitated deterrence, cyberspace below the threshold of war precludes deterrence and necessitates persistence. We must understand this space as a wrestling match in which we are in constant contact with the adversary and we are grappling to sustain the initiative through both our knowledge of what the adversary is likely to do and through our action anticipating what they wish to do.

How should our posture be improved to combat the threat of future Russian interference?

First, we need to build a posture focused not just on Russia, but on revisionist actors across the globe. We need to focus on the effects on our national sources of power we wish to prevent. To achieve this outcome, we need an alignment of forces, capabilities development, operational tempo, and, critically new authorities and decision-making processes that allow the Department to gain tactical, operational, and strategic initiative, continuously. We must operate in cyberspace globally and continuously, seamlessly shifting between defensive and offensive tactics to create an operational advantage—i.e., cyber initiative. By understanding our own vulnerability surface better than our enemies do, we can through resiliency and defending forward render much of their activity inconsequential. This can in turn help free our forces to focus on the truly consequential potential of strategic action below war, to disrupt and disable their cyber activities, creating enough tactical friction in our adversary's operations to shift their focus toward their own vulnerabilities and defending their own networks. This can produce a strategic effect for us.

This will also require a new alignment with the private sector that makes a clear demarcation around protecting human speech. Bots cannot be afforded First Amendment rights. Trending on social media must reflect human majoritarian aggregation, and automated manipulation of that speech needs to be examined in our public policy. The Department should be enabled to disrupt foreign attempts at technical manipulation. 2016 was the Stone Age relative to the sophistication of cyber activities we are likely to see. Before the next presidential election, for instance, we will lose the capacity for audio-visual authentication due to Artificial Intelligence manipulation. We need policy changes to make the Department's capabilities more relevant to the private sector's defense.

What can the Department do to close the gaps—across the federal government and between state and local governments—that inhibit the protection of election infrastructure?

First, it is critical to recognize that there are gaps and that our adversaries are likely to engage in operations that exacerbate them. These gaps exist in the authorities, roles and responsibilities that we have put in place for protecting the voting infrastructure, and exist in the absence of a plan for protecting the information space so that the competition of election campaigns can be conducted fairly by Americans. Based on open source reporting, most State election boards have not prioritized security based on open source reporting and we have not aligned with the private sector social media platforms to produce a coherent plan of how Department resources could contribute to the nation's defense. Our current policy framework essentially rests on a reactive context. The Defense Support to Civil Authorities has not been construed in a proactive and on-going context of defense, which is what is needed to map to the realities of cyberspace. We cannot succeed with an emergency management/disaster relief/crisis framework that places us on the back foot and relegates action to 'cleaning up on aisle nine.' We need to consider authorities that allow DoD, DHS, and our intelligence community to employ a coordinated strategy of cyber persistence as described above. If one considers the approaches emerging among all of our allies, particularly the British, Germans, Australians and Israelis, they are all moving toward increased policy and organizational coordination and synergy. They understand that the answer to the challenge of interconnectedness is not segmentation of roles, responsibilities, and authorities but synergies across pockets of expertise. The policy framing question you should ask yourselves in every discussion you have is whether the policy under question advances synergy or segmentation. If it is the latter it should be rejected; if it is the former it should be explored. Right now our approach to defending our electoral integrity rests on the principle of high segmentation. That will expose us to clever adversaries moving forward.