A Case for Action: Changing the Focus of National Cyber Defense

Rob Schrier

The United States government has made major strides in the past year in improving our nation's cyber defense with initiatives such as the creation of the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and the new DoD Defend Forward policies. However, our nation's emphasis remains focused on improving collaboration and synchronization primarily to improve reaction and response to a cyber incidents and attacks. We must change the goal to move our emphasis to the "left of boom," to create processes and capabilities to prevent, deter and preempt cyber-attacks against our critical infrastructure, as well as interdict and counter those attacks as they are unfolding. We need to regard response as our last resort. We must create a transformative effort to focus speed, agility, unity of purpose, and early warning and to fully incorporate private industry and other partners. Equally important, we cannot revolutionize cyber defense without including an emphasis on defending our democracy, our society and the truth itself from cyber driven influence attacks. I propose the creation of a national level 24/7 cyber defense operational capability with an initial pilot operation focused on defending our democracy in the U.S 2020 elections.

So is our original goal possible? Can we move our cyber defense largely "left of boom"? Can we defend against influence attacks? Can all this be practically achieved? Yes, we can decide to dramatically improve the defense of our critical infrastructure and defend our democracy within our existing laws and policies in a more preemptive and effective manner. We must feel a sense of urgency to accomplish this. This is not a philosophical discussion based on the assumption that the wolves could reach our gates. Because we have ceded our adversaries too much access, the wolves are already inside our gates. Our adversaries have been, are now, and will be conducting increasingly bold and sophisticated attacks against US critical infrastructure and our democracy. We have every reason to expect these cyber and influence attacks will grow more serious. The increasing risks to democracy and, more broadly, to our way of life are too worrisome to ignore.

© 2019 Rob Schrier

Mr. Rob Schrier is currently the Chief of Staff of Asymmetric Operations Sector of Johns Hopkins Applied Physics Laboratory. He leads research on military cyber and Information Operations. He moved to the Laboratory after retiring from the DoD Senior Executive Service after a thirty-six year career. He served as the Deputy to the Commander, Cyber National Mission Force (CNMF), U.S. Cyber Command. Mr. Schrier was a plank holder on the team who established U.S. Cyber Command and served as the initial Deputy Director for Current Operations. Throughout his career, he held a variety of DoD leadership positions after beginning his career as an analyst. Mr. Schrier has more than ten years' experience as a leader in cyber operations. Mr. Schrier earned a Bachelor of Arts Degree from the University of Maryland, a Master of Science Degree in Applied Behavioral Science from Johns Hopkins University and attended the Chairman, Joint Chiefs of Staff CAPSTONE Course.

We need to create a national level 24/7 cyber defense operational capability to change this paradigm with the creation of the National Cyber Operational Defense Cell (NCODC). Names matter. This activity is national in nature. It is cyber in nature (which incorporates influence). It is bound by operational activity and focused on defense. Finally, the word "cell" denotes that this is a lean rather than monolithic function. The NCODC will give us the speed, agility, unity of purpose, and operational connection with private industry and other partners that will change the current paradigm with our adversaries and allow us to gain an upper hand. The NCODC can successfully work on a practical level. So, let's start with what the NCODC will do:

- Direct and synchronize operations to prevent, deter, preempt, interdict and counter adversary activity through a 24/7 operations center that will include operational level participation by key U.S. Government players as well as "authorized to act" Critical Infrastructure private industry representatives. This organization will be operationally focused on defensive actions including executing defend forward actions. This is a not an organization designed to expand into a policy organization or replace other functions in the individual government agencies or the military. The sole goal of this cell is to achieve speed, agility, and unity of effort in defending our nation against cyber-attacks and trying to move the bulk of that defense "left of boom." Individual government elements (such as U.S. Cyber Command and FBI) would bring their authorities and execute their own operations but under the timing and tempo directed by the NCODC Director. There will be thresholds to establish what level of operation fits into this process.

- Drive improvements in both actionable early warning and near real-time intelligence to drive our cyber operations. Utilize publicly available cyber data in addition to classified intelligence to provide the early warning needed to enable our forces to prevent, deter, pre-empt, interdict, and counter cyber and cyber driven influence attacks.
- Lead the cyber interagency and foreign partner process for imminent and ongoing operations.

There are reasons why creating this new cyber defense function will be daunting:

- The NCODC may initially be unpalatable to stakeholders in government and military cyber organizations and these cyber organizations may initially be against the concept.
- The U.S. Government is historically inefficient at creating new organizations.
- The private sector may see the NCODC as both government mission creep into private sector business and a further risk to our civil liberties.
- There is no real US precedent for a continuous 24/7 national level operational activity of this nature.
- Most Americans still do not recognize the seriousness of the cyber and influence threat to our nation.
- There may be a perception this will be a high cost.
- This will take a high degree of non-partisan political will not prevalent today.

Why this could fail:

- Partisan politics may not allow the idea to gain traction.
- The new organization may not survive political infighting by the contributing organizations.
- The selected NCODC leadership may not be bi-partisan or apolitical.
- The private sector may decide against active participation.
- Most likely, there will be enough political will to create the function in a limited fashion, but the compromises agreed to during its mission formulation may dilute it from a 24/7 operational activity to yet another collaborative body where each contributing element continues to act independently, thereby defeating the original goal of speed, agility, and unity of purpose.
- The NCODC will weaken into a synchronization and not exist as an operational cell.

How we can succeed:

- We will achieve efficiency and save most of the cost by not creating a new organization from zero.

- We will name a leadership team and small stand-up strategy team with operational DoD, FBI, DHS and IC participation. We will have the top NCODC leadership focused on operations. These leaders must be perceived by all as nonpartisan and apolitical.
    - The Director will be a political appointee who has real experience in military cyber, government cyber, and in the private industry, but has remained apolitical.
    - The Commander of U.S. Cyber Command Cyber National Mission Force (CNMF) serves as the Deputy Director in a dual-hatted role.
    - The DHS NCICC Director will also serve as the Executive Director a dual-hatted role.
    - An FBI Cyber leader will also serve as the Director of Intelligence in a dual-hatted role.
    - A special Counter-Intelligence leadership role will be created for a CIA representative.
    - Create an industry advisory group (authorized to act) who is fully cleared to work in the Operations Center. This will be the difference maker and will take additional thought beyond this article.
    - Do not create a new, costly operations floor. Initially house this new effort either in existing DHS or U.S. Cyber Command Joint Operations Center spaces.
    - Start with modest funding and increase funding annually.
    - Using a structure akin to a J-Code structure should create staffing efficiency and effectiveness.
    - Most importantly, initiate this new function starting with the 2020 elections pilot activity.

NCODC Pilot Activity: Defending the 2020 Elections

- Create a pilot activity beginning in Fall 2019 to lead the coordinated cyber defense of our 2020 Presidential and Congressional elections across the cyber influence spectrum. This will be an initial, specific, bound activity where speed, agility, and unity of effort will be crucial to our success. The pilot operation will give us the best opportunity to change our focus from responding after attacks to preventing, deterring, and preempting, interdicting, and countering cyber-influence attacks against our democratic processes. Our adversaries will undoubtedly have increased their aggressive intent for the 2020 elections, and we want to be postured to meet them as far "left of boom" as possible. We should stand the initial pilot activity up immediately and build the full NCODC as I prescribed.

Personal Qualifier – These thoughts were written by Robert A. Schrier, retired DoD SES, on a voluntary basis as a retired DoD employee. These are his personal views and do not reflect the views of the DoD, the USG or his current employer, Johns Hopkins Applied Physics Laboratory.