Ally or Die: The Unlearned Joint Organizing Lesson and Key to Survival

Timothy J. White

Joint is better than single service; allied is better than alone; coalition is better than isolation. Neither the United States nor its allies are currently where any would want to be or should be operationally; none are as secure or assured as they should be; and none are performing as efficiently or effectively as required. Given the gravity of national security and the pace of cybersecurity, neither is served by an avoidance of a new call to joining forces in cyberspace. History has repeatedly shown the value of having allies in a tough fight; cyberspace presents that tough fight today.[1]

We can certainly use allies now – across government, private sector, and state partners. The unlearned lesson, however, is that we must organize across common principles and capabilities to create effective alliances for the cyber fight. There is little alternative to going forward: we must learn to ally or we will die. This essay offers learning building blocks, organizing principles, and some concrete future lessons to help cement the effectiveness of cyber allies across the like-minded democracies.

Baseline Building Blocks for Learning Hard Cyber Lessons

The lack of a shared foundation is part of the unlearned lesson. A foundational cyber baseline requires a series of shared and understood building blocks integrated from the beginning in the relationships among allied partners.

Building Block One – Recognize Cyber's 'Overwhelming' Character

Cyber begins at overwhelm. Conventional military kinetic operations are both discrete and linear, and their kinetics are measurable and discernible. While these operations can certainly happen in parallel and together, they generally tend to unfold before they overwhelm. Cyber is experienced more simultaneously as something more ubiquitous and exponential.

Timothy J. White A 30-plus year national security practitioner, strategist, and cyber operations expert leading joint military formations and combined intelligence community organizations. He has commanded at all levels within the Navy and Joint Service, most recently as United States Fleet Cyber Command / TENTH Fleet / Navy Space Command, and previously the Commander, United States Cyber National Mission Force. A former Director of Intelligence for US Indo-Pacific Command, he has served globally in combat zones and conflict areas supporting competition dynamics. He holds diplomas from the U.S. Naval Academy, Naval Postgraduate School, Naval War College, and National Defense University, among others. A former CINCPACFLT Shiphandler-of-the-Year, he misses his days driving a Battleship. He is committed to talent management because up-gunned organizations are made up of up-skilled people. He assesses we are in a race condition, no longer possessing the luxury of time, distance, and accepted international standards as great power competition accelerates.

Building Block Two – Recognize Cyber's Systemic Challenges

Cyber possesses an uncommon degree of persistence, simultaneity, and asymmetry, which is often described with both frustration and good humor. In a graphic novel, a senior military commander or civilian policy maker would say "cyber" followed by a lengthy string of emotive characters – @#$%&!– or grawlix. Six aspects are essential to the shared learning in this building block:

1. **Cyber.** Cyber is analogous to a wild card placed in a search string; anything can be prefixed, appended, or free-associated with cyber and cyberspace. More bluntly, cyber can be distilled down to two data groups that have to be understood. These are the sources and analytics that work with algorithms and aggregators, and the deciders, who are normally human, but increasingly could be artificial intelligence.
2. **Ecosystem and Environment.** Cyber must be considered from at least two basic perspectives: the technology ecosystem and the decision-making environment. The technology ecosystem is the combined hardware infrastructure, firmware, and software that build and connect cyberspace. The decision-making environment is how people, and organizations of people, decide and do – or interact – with and within cyberspace.
3. **Simultaneously Fast and Slow.** Even considering *c* - the speed of light - that governs the top limit of cyberspace campaigns, activity in cyberspace physically can occur impossibly fast. Conversely, given lags in people's responsiveness, it can take a comparatively large amount of time to arrive at a tipping point where action happens. If one has credible and responsible state actors employing a professional target systems approach with a regard for concepts like law of armed conflict and professional trade-

craft, then it still takes many months, perhaps years, of analysis, preparation, movement, and maneuver to execute an exploitation campaign such as the 2020 SolarWinds campaign or the 2021 Colonial Pipeline ransomware campaign.

4. **Attribution and Intent Uncertainty.** Uncertainty over intent or attribution favors the authoritarian or criminal attacker. Bound by a rule of law, democratic defenders will moderate their responses to match the lack of clarity about whether anonymous activity is effective targeted advertising or espionage. Furthermore, both activities could be precursors to a campaign of disruption or destruction.
5. **No cybersecurity but for cryptology.** The national security profession must embrace this mantra as fact. We design, build, and need our national security-related platforms and infrastructure to be secure and available. We are connecting at a distance in order to command/control our military forces in their operations, which requires mission security, assurance, and confidence. These require alignment with, and attachment to, a nation state intelligence community's cryptologic capability; otherwise there is no cybersecurity.
6. **Trust and Identity.** This is about people and their cyberspace interactions with each other, and about the citizens of a country and their agency alongside the sovereignty of a nation and its security. Neither persons nor nations can be taken at face value without confidence in who – and what – is being represented. This is also about trusting our digital identities, which rely on cryptology. Block-chain technology allows for anonymous but highly assured and transparent transactions. Whether that same technology can be leveraged for greater trust in international agreements and alliance remains to be seen.

Building Block Three – Recognize Cyber's Connectivity Pressure

There is only one network, separated in time, which is all connected and inter-connected. Even air-gapped or stand-alone networks will connect to people over time. The tendency to diffuse and connect is the value proposition behind the network effect, which is fundamental to basic information theory. It may take years, but the entropy of the system will drive a logical connection even among those securely separated. This inevitability defines the operating terrain and influences the concept of operations.

Building Block Four – Recognize Cyber's Provenance Dependence

Supply chain and kill chain – don't leave home without 'em. These terms are keyed to a military frame of reference, but you could replace "supply" with "manufacturing" or "research" and "kill" with "market." Whatever your enterprise, it needs to mobilize and aggregate capacity and capability and then deliver to market those goods and services. In a data-driven cybered world, the separation between origin story and end game is governed by the same dependency and vulnerability. If a secure supply chain is lost, then you have handed adversaries advantages throughout their kill chain and crippled your own defense.

In sum, allies need to share similar views of these building blocks to create alliance-friendly organizational designs for national cyber defenses. Intentional organizational definition, structure, and alignment will be our best enablers of success in the unfolding great power competition in cyberspace.

Defending Alone is a Fool's Errand

Joint organizing is key to cyber survival. The term "ally" applies to both inter- and intra-governmental arrangements, which must have sockets for myriad stakeholders to plug into. In this case, the "plug-and-play" aspect of cyber alliances or joint operations becomes an inter-organizational "plug in and help defend" innovation. Like-minded democracies and their constituent organizations must strenuously and jointly learn to design and build their organizations to act on the following tenet: *ally or die*.

Consider the term "ally." It means more than partner or convenience. It means more than integrated operations from planning through execution. It is about establishing common cause with the force of treaty and the consequential power made of binding shared interests and actions. There are plenty of bureaucratic forces and externalities that serve to separate, isolate, and diminish effective security and resiliency; allied causes serve to counter and mitigate these forces. The desired outcomes of coherent strategy, underpinned by allied operations that connect joint forces, public-private partnerships, and the international sphere, are increased capacity and capability; efficiencies in managing escalation and minimizing destabilization; and a dynamic, anticipative posture that capitalizes initiative and sustains momentum. There is agreed consequence and accountability.

To be clear, allied does not mean "the same." Everyone does cyber differently. There is value in this diversity when like-minded partners and stakeholders agree to optimizing principles in pursuit of common cause. One only has to look to the lessons learned from the US approach to joint organization in cyberspace for cyberspace outcomes, which include resilience, security, assured data, and platforms. In this example, military cultures as old as the US Army and Navy - 245 years so far – are now operating alongside the newest Space Force with a displayed unity of action that is both extensible and scalable.

Seven Principles of Organizing with Allies

Mutual cyberspace interests such as national postures oriented on strategy, economic mobilizations, and critical infrastructures coupled with structured, integrated campaigns can be jointly aligned when organizations built on the baseline building blocks continue to observe the following seven cyber and allied organizational principles:

1. **Organize Around Maneuver Principles** – fast and agile. You must think left of reaction and move left of response. In cyberspace, there is no other winning proposition.
2. **Organize for Purpose** – confident, contextual, and frictionless decision making. Cyber moves too quickly for indecision and doubt.

3. **Organize to Generate Outcomes** – enterprise decision making and campaign actions with continuous feedback that sustains dynamic innovation.
4. **Organize to Strengthen Relationships** – culture, behavior, communication, and trust.
5. **Organize to Achieve Common Cause & Shared Goal** – I heard a likely apocryphal story about President John F. Kennedy visiting NASA headquarters for the first time that underscores this principle. During the tour, the president introduced himself to a janitor and asked him what he did at NASA. The answer was simple and clear: "I'm helping put a man on the moon!"
6. **Organize to Generate/Sustain Capacity and Capability** – humanity is living in an increasingly connected, exponentially time-consuming, and attention-deficit disordered world that has nowhere to go but "up" and "more." The world population when the Internet was invented was 3.6 billion, and the number of connected devices was in the single digits. The world population today is more than 7.7 billion, and the number of connected devices today numbers at 13.8 billion, likely approaching 30.9 billion in 2025.
7. **Organize Around a Strategy** – following two decades spent fighting the Global War on Terror and other hot zones, we are now operating under the Great Power Competition strategy of "2+3." Published in 2018, this strategy was of inestimable value. It oriented the executive branch of government, clearly articulated the case for shared interest to allies and partners, underpinned U.S. Cyber Command's (USCYBERCOM) defend-forward and persistent engagement campaign planning; and codified the military services force generation around information warfare. The 2020 Cyber Solarium Commission report, alongside the 2021 establishment and confirmation of the National Cyber Director position, are consistent with recognizing the value of a national strategy. Organizing with allies need just such a clear common strategy as well.

Taken together, these principles enable a unifying multi-stakeholder/organizational/national cyber operational strategy that accounts for respective national interests and goals alongside varied means, and generates an enhanced and collective cybersecurity that ranges from situational awareness to shaping for deterrence.

Five Lessons for Cyber Allies

The better the allies succeed with organizational designs, the closer they will be to having *features over bugs in the national cyberspaces that each will have*. The question will then be how to get closer to optimizing the organizations for defense with respect to boundary conditions of time, terrain, and lethality thresholds, as well as defining conflict categories, adversary numbers and tradecraft, scale imperatives, and the full picture of concrete-to-code-to-context cybered systems.

First, *boundary conditions need to be integrated into allied operations*. Time horizons embedded into allied activities need to be "now through over the horizon," with an understanding of lessons from the past. Terrain lines need to be determined to avoid an incomplete view of compute and cloud. Where does compute happen and where does cloud reside? Or do they reside in the same place? Drawing that line with full allied agreement will allow for more comprehensive strategy development, resource allocation, and decision making. Lethality boundaries need to go beyond the simplistic. For example, drone warfare is not possible without cyberspace and has become a standard tool of modern conflicts. Avoiding complete autonomy is a choice a state makes. However, given the emergence of "full-take" data and "line-speed" decision making, it will be hard not to choose autonomy and automatic if the intent is to achieve maximum effect in cyberspace and kinematic maneuver. Whatever the choice about autonomy, it must be one in which allies commit to operating within the defined boundaries to their fullest extent.

Second, *conflict categories require allied consensus*. Jointly agreeing, deciding, and organizing in advance around conflict in cyberspace will be vital given the simultaneity of time compression and dilation across cyber operations. Consensus will help overcome the difficulty in applying concepts like conventional or strategic deterrence to cyberspace, as well as achieving the systemic benefits in defend-forward persistent engagement. Furthermore, it will enhance an allied nation's ability to manage conflict confusion and escalation by addressing definitional or circumstantial conundrums such as determining what is offense or defense or espionage, if cyber is part of a maneuver warfare campaign, and if there is an existing, recognizable structure. Allied lack of consensus enables the adversary, as a disruptor or spoiler, to diminish or confuse vital interests and reduce allied effectiveness by promoting distorted benefits in sovereign independence and fragmenting allied morale and trust.

Third, *adversary numbers, scale, and tradecraft trajectories* are advancing across the board and require the full spectrum of allied collective attention. Adversaries can be said to be winning the features vs. bugs contest against like-minded democracies whose *bugs (gaps)* are their *features (benefits)* and conversely, their *features (such as strategic coherence)* are the allies' bugs (shortcomings).

Fourth, *organizational alignment and a shared understanding that promotes collective action* is the surest way to address the challenge. A comprehensive target list of adversary campaigns exceeds the scale of any single nation to accommodate even with the best capabilities.

Fifth, *very little across the "Cybered – Cyber" spectrum* spanning the concrete to code to context in the physical, logical, and social world, is truly isolated. The allies must collectively build in security from the beginning and from the ground to top floors of all organizations; ensure integrated visualization and situational awareness; and effectively orchestrate a deliberately structured decision autonomy at machine speed.

The landscape now is more convoluted and distorted than ever. An alliance of problem-solving efforts and decision making within and across governments, alongside our international and private sector partners, is the only way forward.

A Few Final Reflections as Lessons for Like-minded Allies in a Cybered World

The following are two general sets of lessons going forward for cyber allies, drawn from a decade spent embedded in cybered conflict during which my thinking on organizational design and implementation changed as I transitioned from establishing the framework for USCYBERCOM to commanding one joint and one service formation responsible for full-spectrum cyberspace operations. This overview of the lessons is intended to further the thinking for the now and future cyber allies.

Practical Reflections for the Near-Term Future

During my first command of a cyber unit, I had some pre-conceived, and as it turns out, mistaken notions. In my 27 months commanding a Fleet and 21 months commanding our Cyber National Mission Force, I confused mass with capability. This first set of reflections details what I learned from my colleagues' observable mistakes and best practices, that could be coupled with organizational principles to improve our cybersecurity and cyber operations at scale.

- **More than Interactive On-Net Operators.** Operators are necessary, but commanders need as many or more endpoint analysts, developers, all-source analysts, product and infrastructure engineers, and targeteers. We need the enablers that make the hacking possible.
- **More than consuming readiness.** Force generation (up-skill and up-gun, then orient to mission, task, and purpose) of the workforce is critical. Building and sustaining a ready and strategic reserve is vital. This requires training and cycles.
- **Mostly offense is wrong.** The fight is more complex and weighted through Network Operation and defense. It is more about cybersecurity and assured command and control. This is what the adversary thinks they can impact.
- **More than cyber.** The fight is "cybered." That term is really about integrated whole-of-nation-plus information operations and information warfare. These are areas neglected or at least atrophied for some time.
- S**mall, dedicated teams count.** Every member needs to be trained, competent, and qualified. The expectation bar needs to approach exceptional, and it is necessary to start cross-training.
- S**mall, cross-functional teams are the most agile, but you need a lot of them.** Because there is a prioritization and reaction problem, there is always a need for more teams. AI will not solve this challenge (yet). One answer is to build highly trained/qualified active-reserve-civilian small teams, sourced from across the services, formed from aggressive and inquisitive recruiting strategies.

Thinking Forward for the Future

In reflecting on circumstances spanning the summers of 2020-2021 and with an eye to the horizon, we possess several bugs that are currently working to the adversary's advantage. It is wholly within our ability to transform them into features that foreclose adversary advantage.

- Understand the *difference between the skills gap and the discovery gap.* We are fairly good at the former because that looks like training. There is a need to get much better at the latter, which is the product of the curious pursuit of the 'new' that is built on a foundation of critical and creative thinking. Education across allies is key. In the US, the Department of Defense should fully leverage USCC Joint Force Provider and Joint Force Trainer authorities to develop an educational curriculum to supplement the unparalleled training pipeline currently producing our cyber warriors and embrace best practices found within industry, the IC, and allies and partner nations.
- *Acquisition cycles and processes* are abysmal for cyber across allies. Success here looks like sustainable multi-year money and risk tolerance. One method for achieving more transparency and effective oversight would be raising the accountability bar on execution and planning enabled by – at least in the US – fast fail flexibility, among other modernizations. Like-minded democracies are saddled with systems meant for steam-powered equipment and are not currently suited for the speed and scale of change in the digital sector.
- Embrace the reality of a *digital disconnect between open democracies and the ability of adversaries to launch* much of the cyber hacking and associated disruption cost from inside the US. Across the allies, one must somehow reconcile this divide. Are there applicable legal structures from other countries that could be adopted as a pilot? Similarly, allies will need to understand and undertake a large-scale domestic effort to raise awareness about mis- and dis-information.
- Reasonably *solve the information sharing obstacle.* There is lot of classification for national security reasons going on in each nation's cyberspace. We need a hard look that assesses the distinction between what needs to be *classified* versus *protected.* This would both focus on prioritized matters and reveal/unleash a new workforce. Consider how the UK NCSC seems to have successfully integrated common cause and information sharing alongside united government and private sector professionals on a shared national cybersecurity mission.
- The cyber alliance ought to adopt *a professional red-team competitive league* approach. It could be as simple as penetration testing systems (code) and facilities (concrete) or contemplating counter-intuitive or unanticipated alternative scenarios in advance (context). Imagine what a "fantasy cyber red team draft" could look like.

In Closing

All of us have time to confront the threat without kinetically confronting the adversary – for now. If we are to ascribe any value to deterrence, we must agree that deterrence requires readiness, resilience, and organization. Given a commitment to rules-based international order and the opacity that cyberspace brings to sovereignty, identity, and trust, the simple reality is that none of us can do it alone. There is increasing scale, value, and capabilities in allied partnerships and shared perspectives. Organizing teams and commands, bureaus, directorates, and agencies with this in mind will preserve our forward-looking decision space. We must collectively bolster deterrence and move from response to a position of our choosing with an improved readiness posture - together.