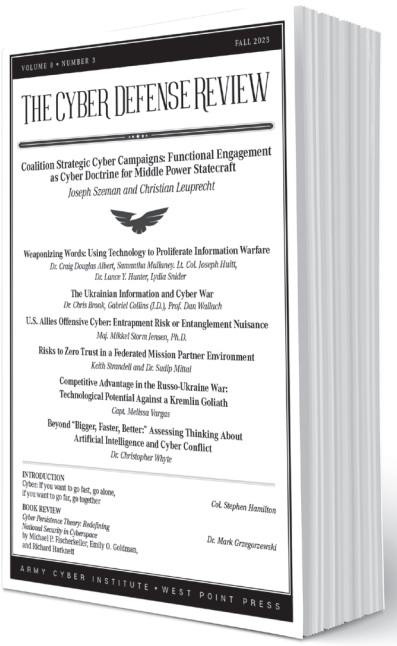
Cyber: If you want to go fast, go alone, if you want to go far, go together

Colonel Stephen Hamilton, Ph.D.



As I write this, Israel has declared itself in a state of war against Hamas. Ukraine pushes steadily for the recovery of its territory from the Russian invasion, and uncertainty around the globe continues to increase. When I reflect on the changes over the last decade in the cyber domain, there appears to be a common theme: collaboration and interdisciplinary teamwork. Technology continues to evolve rapidly. However, our ability to employ technology and defend cyberspace successfully has increasingly required collaboration and teamwork; hence, we cannot do it all alone. Just as in the post-WWII era other manufacturing economies stood up and began to compete with American dominance, so too has American dominance in the cyber domain begun to erode as other nations with different skills and technology emerge as global leaders.

The U.S. Army does nothing alone. Through the doctrine of Unified Action, the different services come together to mass effects, divide responsibilities, and share intelligence and other resources – all with the objective of fighting and winning the nation's wars in land, maritime, air, space, and cyberspace. As a computer scientist and Signal officer, I focused the first part of my career in the physical dimension of computer hardware, software, and networking. Once I transitioned to the Cyber branch, I realized that the

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

COL Stephen Hamilton is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. In his position as Director, COL Hamilton leads a multi-disciplinary team of military and civilian scholars who provide advisement and research for the U.S. Army. He has a B.S. in Computer Science from USMA, an M.S. in Software Engineering from Auburn University, and a Ph.D. in Computer Science from the Johns Hopkins University. COL Hamilton additionally teaches Cloud Computing in the Department of Electrical Engineering and Computer Science. He began his career as a signal officer and deployed in support of Operation Iraqi Freedom in 2004 where he commanded Alpha Company 57th Signal Battalion. Following a tour at USCYBERCOM, he transferred to the Cyber Corps. He holds an extra class amateur radio license, and his research interests include software-defined radios, cloud computing, and data visualization.

cyberspace domain cuts across all three dimensions: physical, human, and information. This is what makes the cyber domain difficult to comprehend and operate in: the academic disciplines that the domain crosses span across electrical engineering, computer science, data science, and social science. It is not enough to be an expert only in computer science—true expertise requires leveraging expertise in all these fields. That is why this trend of collaboration and interdisciplinary teamwork has emerged—the only way to have the expertise in all the fields is to build a team of experts. It is not sufficient merely to be an expert on databases or networking—modern threats are crossing multiple areas of expertise and moving rapidly as the law and the military work to keep pace. As an example, advances in large language models require knowledge not only of advanced math but also of how the very messy real world is encapsulated into data.

In this edition of the CDR, the reader will find several articles that present this theme. Beginning with our research articles, we see the theme of teams of interdisciplinary experts coming together to tackle hard problems. In the article "Civil Cyber Defense," Dr. Mark Grzegorzewski, MAJ Margaret Smith, and Dr. Barnett Koven discuss the concept of a civil cyber defense force like the Air Force's Civil Air Patrol and argue for a whole-of-society approach to cybersecurity. The authors base this recommendation on Estonia's Cyber Defense League (CDL) organization. It not only demonstrates the need for collaboration and teamwork in our society but also shows that our partners in Estonia can potentially help us learn how to do this. There is another article "Risks to Zero Trust in a Federated Mission Partner Environment," by Keith Strandell and Sudip Mittal, which discusses how to share data effectively and securely through federated mission partner networks in a zero-trust environment. In "Coalition Strategic Cyber Campaigns: Functional Engagement as Cyber Doctrine for Middle Power Statecraft" Prof.

Christian Leuprecht and Joseph Szeman provide functional engagement as a strategy for middle power states to operate with a voice in cyberspace since they do not have the capacity for persistent engagement. Yet again, this idea shows the teamwork nature of cyber.

To survive in cyberspace, we must also ensure the various agencies and military units within the Department of Defense work together as a team. The article "Weaponizing Words: Using Technology to Proliferate Information Warfare" presents the risks the US is facing in the information advantage environment. One of the policy recommendations is for the US to unify its approach to data, intelligence, and information warfare. This requires an interdisciplinary and teamwork approach for the US to gain an advantage in information warfare.

We feature two research articles that examine the Russia-Ukraine conflict, "The Ukrainian Information and Cyber War," by Chris Bronk, Gabriel Collins, and Dan Wallach, and "Competitive Advantage in the Russo-Ukraine War: Technological Potential Against a Kremlin Goliath," by CPT Melissa Vargas. CPT Vargas's work describes how collective efforts outside Ukraine (international teamwork) gave the nation an otherwise unanticipated competitive advantage by rallying the world to its cause and ensuring support in actions and weapons, and not just words. In "The Ukrainian Information and Cyber War," the authors discuss the advantages Ukraine had due to cyber threat intelligence from Microsoft and Google, along with the Starlink network to provide connectivity when the Viasat modems were cyber-attacked. This collaboration shows promise but also the risks of efforts between US private companies and the government of Ukraine. These last two articles are real-world examples of how future wars will be fought—it is not just by the Army, but an international teamwork event across the five domains in three dimensions: physical, informational, and human.

Finally, the professional commentary "CISA – The Future of Cyber Weather Forecasting," LTC John Childress describes CISA's Joint Cyber Defense Collaborative (JCDC), which aims to partner with private cybersecurity companies to help disseminate and enhance cybersecurity data to provide a "forecast" for everyone in the cyber ecosystem. He then compares it to the National Weather Service (NWS), which provides forecasts using weather data. The analogy of weather and cyber events was conceived as early as 2000 when the SANS Institute stood up the Internet Storm Center. However, the idea of looking at how the NWS operates to help define how the JCDC will work brings up the theme of collaboration and teamwork. The NWS relies not just on distributed sensors, but also on people to working together to help build an accurate forecast.

I hope the main takeaway from this edition of the CDR is how robust cyber expertise sits at the intersection of other disciplines, and to truly excel in this space, it requires teams of experts working together, sharing knowledge, and leveraging information to fight and win the nation's wars. The future of success in both cyber activities and war resides in collaboration and teamwork as new technologies rapidly emerge and become a part of our new way of operating.