CISA – The Future of Cyber Weather Forecasting

Lieutenant Colonel John Childress

Cybersecurity is like the weather on a summer day; you can see out of your window—just like you can see into your network—but you can't see the storm on the other side of the mountain without a network of stations reporting what they can see. This analogy could be useful in thinking about forecasting for cybersecurity. This approach to cybersecurity—developing a "cyber-weather forecaster"—would enable defenders to see, predict and deal with threats in the same way that the National Weather Service (NWS) forecast helps us decide whether to bring an umbrella or leave it at home. As CISA's Joint Cyber Defense Collaborative (JCDC) matures, developing "cyber weather forecasters" would provide an important improvement in gaining visibility into our networks and conducting predictive analysis.[1,2]

CISA founded the Joint Cyber Defense Collaborative in 2019 to combine the "visibility, insight, and innovation of the private sector with the capabilities and authorities of the federal cyber ecosystem to collectively drive down cyber risk to the nation at scale."[3] In 2021 alone, the JCDC and its 21Alliance partners worked together on major issues including Log4Shell, Daxin and Russia-Ukraine.[4,5] These are major achievements and they represent major milestones; however the JCDC must dramatically improve to provide the U.S. with the tools necessary to deal with more than a fraction of the 847,376 attacks reported just to the FBI's Internet Crime Complaint Center in 2021 alone.[6,7]

John Childress is an Army Lieutenant Colonel who has served in various capacities at U.S. Cyber Command, the Cybersecurity and Infrastructure Security Agency, the Department of Social Sciences at West Point, the Army staff and as a ground commander in Iraq and Afghanistan. LTC Childress currently teaches at the United States Naval Academy in the Departments of Political Science and Cyber Science.

Why the JCDC Will Do for Cybersecurity What the NWS Does for the Weather

The National Weather Service could point the way forward for maturing the JCDC. This opportunity exists as a result of the deep similarities between the missions and functions of the NWS and the JCDC. Both seek to provide a public good—weather forecasts and cyber defense insights—to empower public-private action on a truly national scale.

Both organizations go about their mission in similar ways by combining public and private data—the NWS gathers data from public satellites and private weather stations, and the JCDC gathers data network information from .gov and from private partners like Microsoft and Mandiant—to create comprehensive datasets.[8] Both organizations then use these datasets to develop insights for their public-private partners—weather forecasts from the NWS and threat trends from the JCDC—which serve as information source, trends and predictive analysis that can support their constituents in guiding preparedness and response actions.

Perhaps most importantly, both organizations seek symbiotic relationships with their private partners—the JCDC wants private cybersecurity companies to help disseminate and add value to its products in the same way that local weather forecasters partner with the NWS to distribute and supplement the weather forecast.

Realizing the JCDC's Forecasting Potential

The mature weather ecosystem—the NWS, public and private data sources, foreign weather services and a distribution system which includes the NWS website, the Weather Channel and local news stations—provide a fully-realized vision for a future cyber defense ecosystem.[9] The mature cyber defense ecosystem would include different actors—private cybersecurity firms, network operators, individual citizens, multinational

corporations, government agencies and foreign partners—operating for both their individual benefit and for the good of the nation as a whole.

To realize this vision, CISA should pay attention to four critical aspects of the weather ecosystem that enable forecasting to successfully function at a national scale. First and foremost, CISA should develop a prediction model that adds value to the data that the public-private partners provide. This requires having access to comprehensive cyber data. However, it also implies more than simply recycling cyber data. The ecosystem should be truly symbiotic with each data provider—such as a having access to the "forecast" so they can make decisions for themselves and something that can be used in the marketplace. A mature cyber defense ecosystem should also have cyber defense forecasts which enable private partners to both supply data and to benefit from a public good in the same way that the local television station both provides weather data and repackages, or supplements, the publicly available forecasts on their nightly newscast.

CISA's cyber ecosystem should provide partners with a common framework for data exchange; in other words, data providers must know that CISA's forecasting models depend upon a standardized set of data elements. In a mature cyber defense ecosystem, each stakeholder would know what relevant network data to provide and in what form. CISA's system should be developed incorporating a variety of tools including zero-trust protocols, machine learning and AI-enabled systems to enable real-time, machine to machine, easy-to-use system for gathering data from public and private partners across the country.[10] CISA could then fuse that information with national assets owned by the U.S. government and with information from international partners.

Lastly, the development of cybersecurity ecosystem would require leadership, support and resources provided by the Federal Government to ensure the proper investments are provided to complement the private sector. This would likely include protocols for incorporating potentially sensitive, proprietary and classified data. A mature cyber defense ecosystem would also require the Federal government plan to provide such leadership, support and resources on a recurring basis, at least during the early years. This would be required to ensure a lasting national capacity for conducting cyber defense forecasting.

The Critical "Programmatic Investments" to Create the Cyber "Forecaster" that We Need

Cyber will need to be able to evolve over time to adapt to the new threats, ecosystem partner requirements, and the evolving environment. At the most obvious level, these forecasts will provide day-to-day information which will enable people to prioritize and allocate their cyber defense resources. Cyber defense companies would need to inform less sophisticated operators about the cyber forecasts and assist them in mitigating their risk; more sophisticated organizations and individuals would hire cyber defense companies to supplement the publicly available cyber forecasts.

However, these cyber forecasts would have long-term benefits which go beyond the day-to-day. Long-term cyber forecasts would assist regulators, insurers and organizations understand risk profiles and incentivize a proper response in the same way that the Federal Emergency Management Agency's Flood Maps guide zoning, regulations and insurance rates.[11] When the cybersecurity ecosystem reaches maturity, then an insurance company would be able to set client rates against a known risk profile.

The second focus area which will help mature the cyber defense ecosystem is developing confidence and certainty about the data framework necessary to model the "weather in cyberspace." In other words, a mature cyber defense ecosystem should allow all partners to understand which data elements are necessary to feed the cyber-weather forecast. The JCDC and its cybersecurity partners do not need to build this framework from scratch as it already operates security frameworks which provide a logical point of departure. Furthermore, a guiding framework would need a central governance authority to guide the evolution of the cyber-weather forecasting model. The National Institutes of Standards and Technology (NIST) would be the logical partner to help forge consensus around a framework.[12]

Thirdly, the Federal Government should build a real-time, simple, machine-readable system to receive and coordinate the public-private data necessary to build cyber forecasts. This system must be adaptable and expandable so that it can adjust to changing reporting technologies— over time this system could accept data from across the world. The Joint Collaborative Environment and other systems may provide this functionality and the technical tools may change over time.[13,14]

Lastly, the government must make the right investments and assist partners in developing their investment priorities. In cyberspace the equivalent to weather satellites and national observatories are the government's telemetry from its own networks (.gov, .mil) and the insights from its intelligence community. In a sense, the governments .gov and .mil networks mirror thousands of individual weather stations placed at strategic points in the U.S. while the intelligence community provides the weather balloons that help identify the location of the jet stream.

Federal networks may not require major financial investments, as CISA has authority over the .gov and the intelligence community has a global mission to collect intelligence of this sort already. Instead, the government would likely do better to focus attention on creating fast, reliable processes for collecting, analyzing, and disseminating partner network and Intelligence Community (IC) data into the cyber forecasting model. The IC would also need to ensure that data sources and methods are protected. Inevitably, this may require some difficult decisions on whether to withhold important data which cannot be disclosed for national security reasons.

A practical example comes from the United Kingdom's (UK) Government Communications Headquarters (GCHQ) public partnership with the National Cyber Security Centre (NCSC)—this is the UK equivalent of partnering the National Security Agency (NSA) with the JCDC.[15] In 2021, the NCSC and its partners "dismantled over 22,000 phishing campaigns hosted in UK IP space, linked to over 142,000, attacks."[16]

The United States requires the ability to understand and anticipate the cyber "weather" in our nation's cyber networks. The newly formed JCDC provides the opportunity—in concert with its cyber partners—to develop the national cyber forecasts of the future. This will be essential as we can be assured that cyber threats will not go away and that more needs to be done to develop a predictive capability.

These are exciting times in cybersecurity; cyber defenders certainly have adversaries worthy of their time. The next logical step in our national cyber defense is to develop a predictive capability that is up to the task.

DISCLAIMER

The views expressed in this work are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. CISA, 2020, "Homepage | CISA," Cisa.gov. 2020, https://www.cisa.gov/.
2. "JCDC | CISA," n.d. www.cisa.gov. https://www.cisa.gov/jcdc.
3. "CISA Expands the Joint Cyber Defense Collaborative to Include Industrial Control Systems Industry Expertise | CISA," n.d., www.cisa.gov, accessed November 10, 2022, https://www.cisa.gov/news/2022/04/20/cisa-expands-joint-cyber-defense-collaborative-include-industrial-control-systems.
4. "JCDC | CISA." n.d., www.cisa.gov, https://www.cisa.gov/jcdc.
5. Joint Cyber Defense Collaborative, 2022, Review of Changing the Cybersecurity Paradigm: A Unified Cyber Defense, February 2022, https://www.cisa.gov/sites/default/files/publications/JCDC_Fact_Sheet.pdf.
6. Internet Crime Complaint Center, 2021. Review of Internet Crime Report 2021. Internet Crime Complaint Center. Federal Bureau of Investigation. 2021, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
7. "Internet Crime Complaint Center (IC3) | Home Page," n.d., www.ic3.Gov. https://www.ic3.gov/.
8. Joint Cyber Defense Collaborative, 2022, Review of Changing the Cybersecurity Paradigm: A Unified Defense. Joint Cyber Defense Collaborative, Cybersecurity and Infrastructure Agency, March 2022, https://www.cisa.gov/sites/default/files/publications/JCDC_Fact_Sheet.pdf.
9. National Weather Service, 2018, "National Weather Service," Weather.gov, 2018, https://www.weather.gov/.
10. U.S. Department of Commerce, NOAA. n.d., "Own a Weather Station? We Want Your Data!" www.weather.gov, https://www.weather.gov/iln/cwop.
11. "FEMA Flood Map Service Center | Welcome!" 2019, Fema.gov, https://msc.fema.gov/portal/home.
12. paul.hernandez@nist.gov, 2016, "Cybersecurity," NIST, June 30, 2016, https://www.nist.gov/cybersecurity.
13. @MarkCMontgomery, 2021, "Making the Joint Cyber Defense Collaborative Work" *Lawfare,* August 6, 2021, https://www.lawfareblog.com/making-joint-cyber-defense-collaborative-work.
14. "*Daily News* | InsideCyberSecurity.com," n.d., Insidecybersecurity.com, accessed November 10, 2022, https://insidecybersecurity.com/daily-news/cyber-solarium-leader-montgomery-cites-%E2%80%98joint-collaborative-environment%E2%80%99-key-piece.
15. NCSC, 2019, "About the NCSC," ncsc.gov.uk, 2019, https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.
16. Phil Muncaster, 2019, "UK's NCSC Hails Another Successful Year of Cyber Defense" *Infosecurity Magazine*, July 17, 2019, https://www.infosecurity-magazine.com/news/ncsc-another-successful-year-cyber/.