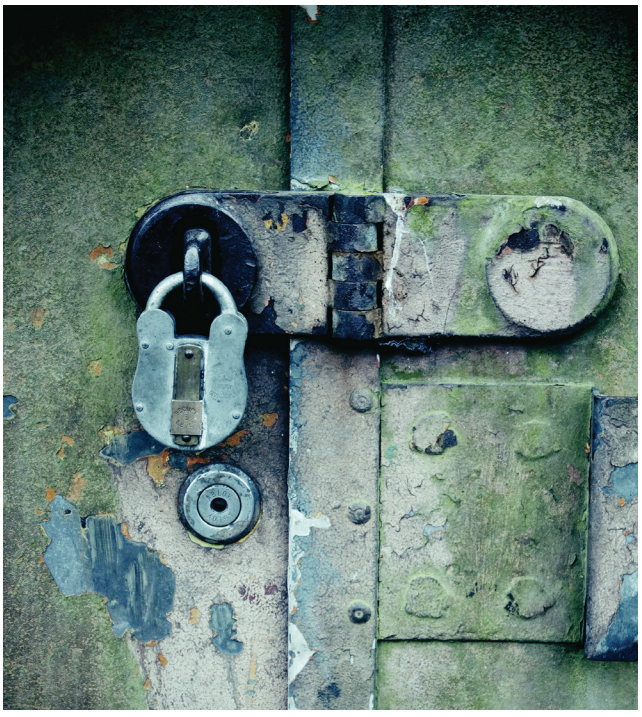

Security Outlook: Six Cyber Game Changers for the Next 15 Years

Alexander Kott and Ananthram Swami, *US Army Research Laboratory*

Patrick McDaniel, *Pennsylvania State University*

Six potential cyber game changers gleaned from a recent long-range planning symposium can help experts identify priorities for future cybersecurity research and development.

Cybersecurity researchers must continually define priorities to help determine which specific areas in the field deserve the most attention and funding. One approach is to look down the road 15 years or so and predict potential disruptive changes that will likely affect cybersecurity. Forecasting future game changers can prove more useful in the long term than being guided by current hot trends.

Earlier this year, representatives from 26 organizations—including multinational hardware and software developers, smaller cybersecurity firms, academic institutions with strong industry ties, and several US Defense Department labs—met in Scottsdale, Arizona, to pool their thinking about such game changers as part of a long-term cybersecurity research planning symposium arranged by the Cyber Collaborative Research Alliance (Cyber CRA; http://cra.psu.edu).

Sponsored by the US Army Research Laboratory, Cyber CRA represents a collaboration between government researchers and a consortium of universities, led by Penn State, to advance theoretical foundations for cyberscience.

These discussions yielded six general areas likely to prove game changers for cybertechnology over the next 10 to 20 years.

CYBER ENVIRONMENT CHANGES

The first two cyber game changers would result from emerging trends in the computing world.

New computing paradigms

Emerging computing paradigms—nanocomputing, quantum computing, biology- or genome-based computing, and so forth, as well as increasingly extreme versions of evolving system and network architectures, such as cloud computing—might, in just a few years, make most current cybersecurity technologies obsolete, thus drastically changing the market.

Quantum computing and networking are already fueling lively debate, with one side making claims for the technologies' inherent security while the other side highlights the opportunities it presents for hacking. Wearables only heighten usability challenges: as user perceptions and behaviors change, so will basic privacy concerns. Such

Published by the IEEE Computer Society

concerns will be compounded as networked computing devices move from augmenting humans externally to invading the body—as prosthetics, exoskeletons, and brain–computer interfaces. The Internet of Things obviously increases opportunities for cyberattack—although, interestingly, it might also offer new defensive approaches as multiple devices could potentially guard themselves collectively.

Biologically inspired computation and communication paradigms—for example, the Gaian dynamic distributed federated database[1]—and related cyberscurity applications, such as artificial immune systems, will attract growing interest, especially as they offer promises for autonomous adaptation to previously unknown threats and even self-healing. However, such complex computing behavior will also bring inherent unpredictability.

New territories for network complexity

An even more fundamental environmental game changer will occur as we cross a network complexity threshold and enter new territories beyond the limits of conventional system manageability, perhaps even stretching human comprehension. Qualitative increases in technological complexity—enormous in size, connectivity, interdependence, heterogeneity, and dynamic capabilities—coupled with the exploding network growth occurring now in underserved communities worldwide might defeat conventional scientific and engineering approaches to cybersecurity.

Right now, the cyberresearch community has little insight to help us observe, stabilize, and control very-large-scale and multidimensional networks. There's still much for us to understand about how social-cognitive and cyber-physical links will govern overall network complexity.

As one symposium attendee put it, "Our products are already far too complex … so complex that nobody in our corporation can possibly fully understand them, and this just keeps getting worse." Inarguably, increased system complexity enhances opportunities for adversarial attack.

TECHNOLOGY TRENDS

Two more cyber game changers will result from technology trends already occurring but predicted to grow exponentially.

Big data analytics

Though still immature from a cybersecurity perspective, big data analytics—predictive and autonomous—is an area already exerting a noticeable influence. Potentially reaching global scale, able to anticipate multiple new cyberthreats within actionable timeframes, and requiring little or no human cyber-analysis, big data analytics is a third game changer that could bring new potency to cyberdefense.

Much of this power will likely derive from aggregating and correlating a broad range of highly heterogeneous data, which is challenging in itself. Add to this heterogeneity the noise, incompleteness, and massive scale characteristic of cyberdata, and the challenges only increase.[2] Much work remains for developing algorithms that can ferret out deeply hidden, possibly detection-protected information from so heterogeneous a mass.

Resilient self-adaption

Potential innovation based on resilient self-adaptation represents a fourth game changer. Cybersecurity in this case will derive largely from system agility, moving-target defenses, cybermaneuvering, and other autonomous or semi-autonomous behaviors.[3] Exploiting such self-adaptation might mean shifting a significant fraction of design resources from reducing vulnerabilities to increasing resiliency.

A truly resilient system could experience a major capability loss due to cyberattack, but recover sufficiently rapidly and fully so that its overall mission proceeds successfully. For example, promising results have been shown for software residing on a mobile phone to perform self-healing—by applying patches or self-rewriting code—in response to abnormal behaviors it detects.[4]

However, effective autonomous self-adaptation calls for a degree of machine intelligence far ahead of what's now imaginable and would also increase system complexity, thus multiplying vulnerability risks. Given that complex attacks, along with their circumstances, are both diverse and unpredictable, achieving practical resiliency is no more than probabilistic—not a comforting thought for future systems operators.

CYBERTECHNOLOGY BREAKTHROUGHS

The final two game changers involve breakthroughs that are perhaps less likely in the next 15 years, but still on the radar.

Mixed-trust systems

The fifth game changer involves new design methods for mixed-trusted systems. We see these as security-minded, flexible, modifiable systems that combine and accommodate untrusted hardware and software—resulting from dubious supply chains, legacy elements, accreted complexity, and numerous other sources—with clean-slate components. Related ideas include a management protocol that applies trust-based intrusion detection to assess degrees of sensor-node trustworthiness and maliciousness.[5]

This game changer depends on qualitatively significant changes in the design methodologies and tools that enable complex systems to be synthesized—for example,

reinforcing untrusted components with clean-slate, highly trusted "braces." Such designs would also have to include components that could be rapidly and inexpensively modified to defend against new threats as they're are discovered. A breakthrough in current formal methods or the emergence of as yet unknown but highly reliable semiformal methods would thus be required.

Active defenses

Our final game changer involves the possible emergence of active defenses against cyberthreat sources: strategy-oriented approaches, offense-based techniques, alternative security postures, and deception- and psychology-aware mechanisms. Currently, little is understood about the shape such methods might take, especially in view of the legal and policy uncertainties surrounding cybersecurity in general, and proactive cyberthreat responses in particular.

Extensive strategic and tactical knowledge developed through long human experience with conventional conflicts might offer important insights about holding adversaries at risk and defeating their will to attack. But focus on the past might also mislead and limit our thinking.

Whatever the details, any such approaches will benefit from greater situational awareness and require understanding our adversaries' architectures, infrastructure, and sensing capabilities as well as we do our own. We will also need languages and models to help clearly and precisely articulate the specific defensive and offensive circumstances, cultural intelligence and adversary modeling, and deep insights into individual and collective cognitive processes.

Considering the rate of change in computing technologies vis-à-vis the long time horizon for these game changers, it would be foolhardy to suggest that all six—or even any one of them—will emerge exactly as we envision here, if at all. However, weighing how these game changers might play out in the future, and paying attention to potential developments that could affect cybersecurity researchers, technologists, and their funding organizations will help prioritize our cyberscience and engineering efforts. C

References

1. A. Toth et al., "Coalition Warfare Program (CWP): Secure Policy Controlled Information Query and Dissemination over a BICES Network," *Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR IV*, T. Pham et al., eds., SPIE Digital Library, May 2013; http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=1691136.
2. A. Kott and C. Arnold, "The Promises and Challenges of Continuous Monitoring and Risk Scoring," *IEEE Security & Privacy*, vol. 11, no. 1, 2013, pp. 90–93.
3. S. Jajodia et al., *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*, Springer, 2011.
4. T. Azim, I. Neamtiu, and L. Marvel, "Towards Self-healing Smartphone Software via Automated Patching," to be published in *Proc. 29th IEEE/ACM Int'l Conf. Automated Software Eng.* (ASE 14), 2014; https://drive.google.com/viewerng/viewer?a=v&pid=sites&srcid=dGFuemlydWwuY29tfHRhbnppcnxneDo3OGE5OTA1NDZhMGQ5OGU5.
5. F. Bao et al., "Trust-Based Intrusion Detection in Wireless Sensor Networks," *Proc. 2011 IEEE Int'l Conf. Comm.* (ICC 11), 2011; doi: 10.1109/icc.2011.5963250.

Alexander Kott *is chief of the Network Science Division at the US Army Research Laboratory (ARL), where he manages a portfolio of research in cybersecurity. Contact him at alexander.kott1.civ@mail.mil.*

Ananthram Swami *is senior research scientist in the Network Science Division at ARL, an IEEE Fellow, and an ARL Fellow. He also manages the Cyber Collaborative Research Alliance (Cyber CRA). Contact him at ananthram.swami.civ@mail.mil.*

Patrick McDaniel *is a professor in the Department of Computer Science and Engineering at Pennsylvania State University, codirector of the Systems and Internet Infrastructure Security Laboratory, and lead scientist for the Cyber CRA. Contact him at mcdaniel@cse.psu.edu.*

Editor: Jeffrey Voas, National Institute of Standards and Technology; jvoas@ieee.org