Cyberthreats in 2025

James Bret Michael, Naval Postgraduate School

Richard Kuhn, National Institute of Standards and Technology

Jeffrey Voas, IEEE Fellow

Computer *hosts a virtual roundtable with six experts to discuss upcoming cyberthreats in 2025.*

In *Computer*, virtual roundtables (VRTs) are virtual panels. We ask a series of questions to a group of experts via email to ascertain their thoughts on a topic du jour. One difference between VRTs and face-to-face panels is that no expert knows who the other experts are. That is different from an in-person panel, where answers from one panelist can affect the responses of others.

In this VRT, our topic of discussion is what the upcoming cyberthreats in 2025 might be. We could have asked about other years, such as 2030 or 2035. However, for this topic, the larger the number, the more the answers become sheer speculation. We believe that distant, futuristic speculation is of little value to the reader, given the relentless hacks that occur daily.

In this VRT, we invited six experts to respond to 12 questions. Their written responses may have undergone minor edits. However, as organizers, we attempted to keep their words as verbatim as possible. The six experts are Jon Brickey (Mastercard), Simson Garfinkel (U.S. Census Bureau), Gary McGraw (Berryville Institute of Machine Learning), Latif Ladid (Université du Luxembourg), Bruce Potter (shmoo.com), and John Viega (Capsule8). (See "Roundtable Panelists" for more information about the panel.)

It is important to note that the opinions of the experts are their own, with no input from the article editors. We hope readers who are concerned with cyberthreats and cybersecurity will find these questions and responses enlightening.

COMPUTER: What will be the prevalent types of cyberthreats in the year 2025?

JON BRICKEY: By 2025, threats will be more automated, more intelligent, more disruptive, and even destructive. Nation-state actors will push the envelope and use cyberattacks against critical infrastructure because they can't achieve strategic effects through more traditional means. We'll also see more of the same on the criminal actors side as they continue to take advantage of an explosion in consumer-focused fintech [financial technology] apps.

Digital Object Identifier 10.1109/MC.2020.2983529
Date of current version: 4 June 2020

ROUNDTABLE PANELISTS

Jon Brickey is senior vice president, Cybersecurity Evangelist, for Mastercard Operations and Technology. In this role, he supports Corporate Security's mission of delivering safety and security at the speed of business. Before joining Mastercard, he served in the U.S. Army and retired as a colonel. Brickey received a Ph.D. in computer science and information systems from the University of Colorado Denver in 2010. Contact him at jon.brickey.@mastercard.com.

Simson Garfinkel is the senior computer scientist for confidentiality and data access at the U.S. Census Bureau. He holds seven U.S. patents and has published more than 50 research articles in computer security and digital forensics. Garfinkel received a Ph.D. in computer science from Massachusetts Institute of Technology in 2005. He is a Fellow of the IEEE and of the Association for Computing Machinery and a member of the National Association of Science Writers. Contact him at simson.l.garfinkel@census.gov.

Latif Ladid is a senior researcher on the Faculté des Sciences, des Technologies et de Médecine, Université du Luxembourg. He is founder and president of the IPv6 Forum and board member of the 3rd Generation Partnership Project since 1999. Ladid received a postgraduate diploma in business administration studies from the Business and Management Institute of Leeds Polytechnic, United Kingdom. He received the 2002 IPv6 Forum Internet Pioneer Award and the 2016 IPv6 Life Time Achievement Award. Contact him at latif@ladid.lu.

Gary McGraw is cofounder of the Berryville Institute of Machine Learning and the author of *Software Security* (AWL, 2006) and 10 other software security books. McGraw received a dual Ph.D. in computer science and cognitive science from Indiana University. He served on the IEEE Computer Society Board of Governors and produced the monthly "Silver Bullet Security" podcast for *IEEE Security & Privacy* magazine for 13 years. Contact him at gem@garymcgraw.com.

Bruce Potter is the chief information security officer at Expel. He is responsible for cyber risk management and ensuring the secure operations of Expel's services. He cofounded Ponte Technologies. He also founded the Shmoo Group in 1996 and helps run the popular annual hacker conference, ShmooCon, in Washington, D.C. Contact him at gdead@shmoo.com.

John Viega is the chief executive officer and a cofounder of Capsule8. He coauthored the Galois counter mode, which encrypts more than two thirds of encrypted web traffic. He has coauthored many books on security, including the first book for software engineers on security. Viega received an M.S. in computer science from the University of Virginia. He has an extensive track record at both start-ups and large security companies. Contact him at john@viega.org.

SIMSON GARFINKEL: Before we consider the cyberthreats of 2025, it's important to consider the likely cyber landscape of 2025, as determined by current trends in technology evolution, policy changes, and the environment in general. Assuming the deployment of technology continues for the next five years, the year 2025 is likely to see increased deployment of partially finished, somewhat buggy, hybrid hardware/software systems in every aspect of our technological infrastructure, with the knowledge that these systems can be patched and upgraded after they are shipped to customers. It will be common for newly purchased, newly deployed systems to immediately perform software updates on first start. This will allow for faster time to market, but the net result will be more computerization with systems that are less mature and less reliable.

NIST defines a cyberthreat as "an event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss." Given the NIST definition and the likely technology scenarios, I suspect that we will see increased attacks with financial and political goals. On the financial side, I expect more theft and extortion. On the political side, I expect more attacks aimed at delegitimizing governments. Those might be information operations, such as those against Facebook and Twitter that have received so much coverage, or attacks against infrastructure with the goal of delegitimizing governments by demonstrating that they cannot protect their citizens. Specifically, I am expecting threats against embedded systems, threats against the accuracy and completeness of information in consumer-facing systems, and the use of cybersystems for intelligence gathering (for example, surveillance and information theft).

Software-related security vulnerabilities will continue to top the most important problems for us to solve, even in 2025.

LATIF LADID: The cyberthreats will still be money oriented, but the political threats (influencing and interfering in the national political systems) will become rampant around the world. New cyberthreats will come also from the zillions of very-low-cost Internet of Things (IoT) devices shipped to the market with zero security, especially in smart cities. Obviously, 5G will enable new higher-speed attacks with massive broadcast attacks. Cryptocurrencies will be also very good candidates for hacking, including government policies to regulate them.

GARY McGRAW: Software-related security vulnerabilities will continue to top the most important problems for us to solve, even in 2025. Although we now know what to do to make software security work, we still have a long way to go in actually doing those things.

Disinformation and misinformation will continue to be big problems in cybersecurity in 2025. Machine learning (ML) vulnerabilities will be a new reality by 2025. If we start working on ML security (MLsec) immediately, we may avoid some real trouble.

BRUCE POTTER: I think we are currently in a wave of commodity-grade attacks around cryptocurrency/cryptomining/ransomware that will largely have ebbed by 2025. For the most part, I expect endpoints and operating systems (OSs) to be reasonably hardened, reasonably patched, and less likely targets for adversaries. I think the focus will continue to move from access (that is, persistence on a host, OS-level access) to data compromise. Data are where the money is; data can be had in big chunks when you find them. I think attackers will continue to look for ways into data stores of interest and find ways to monetize them if they're cybercriminals or use them for intelligence operations if they are nation-states.

The other threat will be around information operations. As the Internet has democratized over the years, the ability for an adversary to leverage various platforms as part of a large-scale information operation has skyrocketed. The attack here is largely nontechnical but uses technical means for execution. Like most attacks, for a little investment, attackers get a huge return.

JOHN VIEGA: The threat landscape will evolve to keep up with the times, but, in some sense, not much will be different. There will be plenty of career criminals looking to make money via whatever is expedient (for example, cryptomining, ransomware, and so on). And then there will be nation-state attackers that are far more targeted, having vastly less day-to-day impact on businesses but a much larger geopolitical impact.

***COMPUTER*:** Which of those prevalent cyberthreats will pose the highest risk to society?

BRICKEY: While criminals will continue to have a negative impact on society (not just via financial crimes but also using ransomware), nation-state threats will pose the highest risk as they disrupt and destroy critical infrastructure.

GARFINKEL: Threats to democratic institutions, industrial control systems (including autonomous vehicles), and the financial sector represent the highest risk to society because they have the power to damage society in ways from which we could not readily recover.

LADID: See my response to the first question.

McGRAW: Since software is working its way into everything we build, all aspects of society are subject to software risk. My view is that building secure software remains the most important immediate focus.

POTTER: The information operations efforts will have the largest impact. We see that today in election security. Puppet accounts and willing media participants result in the ability for misinformation to spread rapidly around the globe. Couple that with a few targeted technical attacks (think: the reporting websites of a few swing counties in Wisconsin, Michigan, and Ohio), and, suddenly, the entire country is in an uproar. Cheap to carry out with an unbelievably large impact.

VIEGA: From a technical sense, while IoT and cloud technologies are going to be growing targets, people will always be the weakest link. The most prevalent, effective, and worrisome threats are going to be nation-state disinformation campaigns—interfering with the elections and the politics of the Western world.

I say Western world because there's a massive and obvious asymmetry that puts the Western world at a particular disadvantage—English. There are nearly 800 million nonnative English speakers in the world, spread around the world, and all fairly highly skilled. But there are fewer than 200 million nonnative Mandarin speakers and about 150 million nonnative Russian speakers. That expertise is not really concentrated in the Western world. Not being well equipped to reciprocate makes it much harder to build enough capability that would lead to some sort of mutual nonaggression agreement. For the foreseeable future, we're quite possibly stuck with subtle but tremendously effective geopolitical manipulations through the media.

COMPUTER: What types of vulnerabilities will be common in the future? Are there any technical advances that portend solving age-old problems, such as those that take advantage of a computer's memory-management systems (such as Spectre and Meltdown)?

BRICKEY: With the burgeoning amount of code designed for the cloud and containerless computing environments as well as the lack of secure coding training/awareness, there are bound to be key vulnerabilities in the future. There will likely be major vulnerabilities discovered in cloud computing that will impact the majority of enterprises.

GARFINKEL: Spectre and Meltdown caught many organizations off guard: they were viewed as fundamentally new kinds of exploits. Given the rate of innovation, we're likely to see yet another fundamentally new exploit before 2025.

Puppet accounts and willing media participants result in the ability for misinformation to spread rapidly around the globe.

More concerning in my mind, though, is improved attacker fluency in exploiting existing vulnerabilities. For example, in 2010, Kris Kaspersky and Alice Chang demonstrated that remote code execution was possible by exploiting bugs in specific versions of Intel CPUs: using these bugs requires that the attacker have knowledge of specific targets, but the bugs are stealthy and the payoff can be huge, because the bugs can't be demonstrated on processors that aren't vulnerable. Like Spectre and Meltdown, these bugs exist because the silicon in the CPU doesn't faithfully implement the application binary interface. Likewise, I expect that increased use of formal methods for defensive purposes is likely to result in increased use of formal methods to find data-dependent exploits.

LADID: Mitigating cyberattacks is a mix of policy and new mitigation technologies. The Finnish STRATCOM regulator is an excellent reference cybersecurity model to be adopted by the countries that can adopt this centralized cybersecurity model.[1]

McGRAW: The future is here, but it is sparsely distributed. Though we have been making technical progress at the bleeding edge, older tech with known problems will still be prevalent in 2025.

POTTER: Vulnerabilities will shift to ones of process versus low-level technical defects. For example, a continuous integration and continuous delivery pipeline that utilizes a public bucket for code or a misconfigured access control list at an integration test provider can give up all your source code without even touching your network. With the continued migration to infrastructure as a service (IaaS) and software as a service (SaaS) providers, even by huge companies, the ability to configure everything in a secure manner becomes far more important than the impact of side-channel attacks on processors like Spectre and Meltdown. Helping organizations understand their new attack surface and how to manage security on hundreds of SaaS solutions is where the next big investment in tech is going to happen. Cloud access security brokers (CASBs) and others aren't going to cut it.

On the host, I think we will continue to see the "drip, drip, drip" of research on Spectre-like attacks. These vulnerabilities are an indictment of the last two decades of chip advancement. We made systems faster by doing everything at once and later figuring out what the right path was. Turns out, that's hard to do without leaking information. I imagine the chip manufacturers will figure that out (much like we've figured out how to deal with differential power analysis and other low-level attacks), but it will come at the cost of performance and economic efficiency.

The rise of surveillance capitalism shows just how clueless most users are when it comes to their own behavioral data. This will get worse, not better.

VIEGA: Processor-level problems will continue to be a ripe source of challenges due to their complexity. But most of them have been, and will continue to be, lightly exploited. Attackers follow the path of least resistance, and there will generally be much easier ways in. People will still be the weakest link, and misconfigurations that lead to issues will be common. Insofar as vulnerabilities go, the continued move away from C and C++ for applications will be a good thing, but we're unlikely to see a decline in good old input validation problems like basic command injection. They're easy to add and often hard to protect against generically.

***COMPUTER*:** In 2025, what will the general public's expectations be for cybersecurity and online privacy?

BRICKEY: Consumers may have more control over the use of their data by 2025, so online privacy expectations will likely increase. By 2025, several U.S. states will have their own privacy laws, and there will be increasing pressure on the federal government to pass a national law. I doubt there will be much higher expectations for cybersecurity, as pervasive IoT makes it more difficult than ever for the public to keep tabs on the security of their devices.

GARFINKEL: I expect that the general public will become increasingly fatalistic about the state of cybersecurity and resigned to the existence of exploitable bugs. I think that such attitudes are problematic, as they are likely to result in decreased cybersecurity funding over time.

LADID: Privacy has been dead for a long time, starting with the yellow pages and loyalty cards. Privacy is very big business. Privacy by design is possible only if it is integrated in the OS. As a case in point, Internet Protocol version 6 (IPv6) has a privacy protocol, unlike IPv4. The Mac address is scrambled so that footprints won't be harvested by web scanners.

McGRAW: The public seems to be completely in the dark with respect to computer security and privacy, especially in the United States. The rise of surveillance capitalism shows just how clueless most users are when it comes to their own behavioral data. This will get worse, not better.

POTTER: I hope the members of the public at large will actually feel like they have some control over their lives and personal data online. As laws like General Data Protection Regulation (GDPR) spread around the world, consumers will feel more empowered to control their data and will have more visibility into where their data are. That said, I believe that most consumers have a general expectation of security and privacy but really aren't equipped (nor should they have to be) to understand it fully. For instance, when installing a video camera that is protected only by a username and password, a consumer should know a) that's not particularly secure and b) don't reuse passwords. But as the recent rash of Ring camera compromises have shown, many consumers don't understand that. It's on companies like Ring to require multifactor authentication to protect consumers, not on consumers to demand it.

VIEGA: People in our society want to feel safe, and if there's not an obvious daily threat, they'll continue to feel that way. I think people will know there's some risk but feel mostly safe and almost wholly unconcerned, whether it's warranted or not.

***COMPUTER*:** What advances in cybersecurity defenses and privacy protections should we be investing in now to address the cyberthreats anticipated to be prevalent in 2025?

BRICKEY: We need to do better at data-centric cybersecurity strategies. We need to see chief privacy officers, chief information security officers, and chief risk officers working closer together for additional protections. Boards of directors will require they do this, and limited budgets will force them to find dual-purpose solutions.

GARFINKEL: Our best defense would be to build systems that have dramatically fewer vulnerabilities. We can do this by significantly reducing our reliance on software written in unsafe programming languages, increasing the use of formal methods, and isolation approaches.

For example, today, compiled programming languages like Go and Rust offer the speed of C/C++ while offering memory and type safety. JavaScript is also fast enough for a large number of applications, as evidenced by the success of node.js. As a result, new projects shouldn't be started in C/C++, and existing code should be rewritten. Sun had an effort in the 1990s to rewrite the Unix kernel in Java: it failed. Sun made two errors: Java in the 1990s didn't offer sufficient performance, and the project sought to redesign the entire OS from the kernel up. Since most cybersecurity problems are in applications and libraries, it makes more sense to start rewriting network servers, system libraries, and command-line tools, leaving the kernel for last. Until then, we should significantly increase the use of automated static analysis tools for existing code.

LADID: Wars have been stopped with peace treaties. Cybersecurity needs peace treaties around the world to first address government threats. This is the biggest task for the next 10 years and even beyond. But we will have still a cold cyberwar for years to come.

MCGRAW: Educating the public about privacy risks and the poor tradeoffs people are making when they use much advanced technology.

POTTER: Data mapping is a huge one. Understanding which data move where in an organization is key, especially as attacks continue to focus more and more on data themselves. To properly implement security controls and have any hope of protecting personal information, companies need to know where their data are. This is easy in small companies but incredibly difficult in large ones.

Also, a general focus on data minimization will help as well. Companies view data as assets because data feed analysis activities and can be used to better understand their products and customers. However, data are also a liability and need to be treated as such. This is an engineering discipline that needs to spread across the industry.

VIEGA: The security industry needs to invest in keeping up with new technology. Most people in the industry really don't get cloud technology, they don't understand containers, and they don't understand anything in the ecosystem of modern software (for example, service meshes). Also, the industry needs to figure out how to do better with embedded devices, since they're becoming ubiquitous and are generally both quite vulnerable and incredibly difficult to keep patched.

***COMPUTER*:** Given that it is hard to predict five years out what information and computing technologies will be ubiquitous, how the systems those technologies are used in will be developed and sustained, and how those technologies will be employed by users of information and communications technology (ICT), how much credibility can we place in educated guesses about what the future cyberthreats will be? Are there too many unknowns?

To properly implement security controls and have any hope of protecting personal information, companies need to know where their data are.

BRICKEY: There are already too many unknowns, and we know that trends in the IoT (to make consumers' lives more convenient) will add to the complexity. There's an app for everything, and that will expand to include autonomous vehicles, robotic assistants, and artificial intelligence (AI)-enabled assistants. Consumers will expect more of this, and companies are more than willing to deliver and gain a foothold on the market.

GARFINKEL: "The future has arrived—it's just not evenly distributed yet." This quotation, frequently attributed to cyberpunk writer William Gibson, can be easily applied to the state of ICT in general. Most of the likely uses of computers and networks in 2025 are already employed today; even the popular apps of 2025 probably exist today in some form.

For example, many people see ransomware as a relatively recent phenomena, but the first ransomware, the so-called AIDS Trojan, was deployed in 1989; a paper describing a more sophisticated system was presented by Young and Yung at the 1996 IEEE Symposium on Security and Privacy ("And there is nothing new under the sun," Ecclesiastes 1:9).

Most of the likely uses of computers and networks in 2025 are already employed today; even the popular apps of 2025 probably exist today in some form.

This is good news for prognosticators: predicting the future is really just an exercise in understanding the present. We can improve our forecasting ability by studying the progress of earlier IT transitions. But it's important to pick your examples carefully. The early history of the Internet looks a lot like the early history of radio, but not at all like the early history of television. I think that this is because both radio and the Internet were conceived and initially deployed as two-way communications systems, but when they went mainstream, they both evolved into predominantly one-way systems for disseminating information.

Looking specifically to cyberthreats, I think that current trends are likely to accelerate and that systems used by governments and major corporations in 2025 will be more restrictive, more locked down, and more utilitarian than anything widely used today, while educational institutions, small businesses, and individuals will enjoy increasingly sophisticated and powerful tools. Balancing productivity and risk will remain a difficult task for security professionals.

LADID: This is a very tough question. However, the Finnish example has shown very good results. It's a good start but needs to invest in mitigating new cyberthreats enabled by new technologies. The speed of hackers is accelerating.

The users are employing new made-easy technologies, such as iPhones, without understanding how they function and how to protect them. I was at a university a week ago, and the university has introduced a computer course for beginners, as the new students do not even know how to use a mouse or a keyboard, let alone go into Windows, as they are used to just swiping on the iPhone screen or using face recognition.

McGRAW: Everyone is a BSer!

POTTER: There are a ton of unknowns. But we're at a point in the industry where we have enough historical data of what global computing habits look like such that we can make more educated guesses than in the past. While we can't predict revolutionary products that will change the world, we can predict roughly how they will communicate, the types of data they will have, and the systems that will be involved. The push toward cloud computing by basically everyone allows us to predict vulnerabilities and controls, even if we aren't sure of exactly the cloud service that will be deployed.

VIEGA: I think it's safe to say attackers will generally follow the path of least resistance. What that path tends to look like will vary based on how the technical landscape evolves and how the security industry evolves. In five years, there are bound to be a few surprises, but it's a short enough time horizon that I don't think we'll be living in a fundamentally different world.

***COMPUTER*:** Cybersecurity guidance typically recommends rapid application of updates and patches, with the implicit assumption that original installs and updates are free of malware. But there are increasing reports of malware contained in code coming from the original vendor, particularly for smartphones. What are the prospects for containing this threat?

BRICKEY: I think we'll see some improvements in this area due to more attention to supply chains and the inherent risk in third parties. There is a growing number of products and processes, like the blockchain technologies, to verify code at inception and throughout its lifecycle; however, this is not likely to be common practice in the near future.

GARFINKEL: The threat of malware and vulnerabilities delivered with vendor software is nothing new: the 1988 Morris Worm spread, in part, by using a "trap door" created for debugging that allowed remote code execution. Ken Thompson, in his Turing

Award lecture, discussed how another back door could be put into the C compiler, although it is unclear if an infected C compiler was ever distributed by AT&T.

It is conceivable that the risk of vendor-supplied malware and back doors might be addressed by using formal methods and proof-carrying code. But this could only work for a very restrictive set of programs whose behavior can be formally specified. Here, it is useful to remember that the definition of a trusted system is one that can violate your security policy: this applies to both software and vendors alike.

LADID: This is incorrect. Microsoft spends a lot of effort to patch its security software holes, and people don't even pay attention to updating their OSs. Same for Apple. Obviously, software is not a 100% science, so it will be always attackable, and the updates should be made mandatory, a tough message to get into 5 billion simple users. Automating updates as Apple does during the night is a good solution, but the device has to be connected and powered during the night. I cannot get this done myself.

McGRAW: There is no avoiding the patch, unless we build perfect software to begin with. Since that's not possible, we'll always be stuck with patching.

POTTER: Pay more money for your products. When things are cheap/free, you are the product. We're seeing this in low-end Android smartphones because the vendors either have poor cybersecurity practices or they are finding other ways to monetize their platform. When companies are properly compensated for the products they make, they have more resources to dedicate to building a higher-assurance product.

VIEGA: Not good. I think back to a story Steve Bellovin told me a long time ago, about a person at Bell Labs who was responsible for a bug so egregious and easy to exploit that he was personally pretty convinced it was an intentional back door. But there was no way to be sure that it wasn't just a stupid error.

Now, take into consideration the trend of systems getting larger and larger based on the number of lines of code, primarily because projects are shifting from "mostly proprietary code and a little bit of open source" to "mostly open source and a little bit of proprietary code." (I've heard people claim that we've gone from 10% of new code being open source to 90% over the last 10–15 years, and that feels right.) There's a lot that can (and will) continue to go wrong here.

***COMPUTER*:** Adversarial images are a popular research topic, but we have not seen real-world exploitation. As autonomous systems become prevalent, how concerned should we be about this cyberthreat?

BRICKEY: We should be concerned about this, but mostly on the lower end of the impact scale—as a nuisance to society. It could be a larger threat as our military systems are deployed around the world and as adversaries share knowledge about vulnerabilities and exploits.

GARFINKEL: Adversarial images, like putting a sticker on a stop sign to make a convolutional neural network think that it's a "speed limit 55" sign, makes for a popular research topic because the results are both dramatic and easy to understand. We haven't seen them in the wild because the cross section of autonomous cars and miscreants is currently quite small. However, the availability of high-power laser pointers has resulted in several pilots being dazzled while they were landing commercial passenger aircraft, so I think that we should be very concerned about all sorts of malicious threats that autonomous systems may face from miscreants.

LADID: I have two European Union (EU) projects: 5G-DRIVE and 5G-MOBIX, where we are addressing autonomous networks, and, indeed, the security, privacy, and cybersecurity issues are not yet comprehended properly, as we need large-scale deployment to assess the new risks coming from the 5G ecosystem around moving vehicles but also from all of the functionalities coming from the vehicles, the multiaccess edge computing side, the backbone, and so on.

It's a huge task, as different standards bodies have to join forces as their standards merge in these scenarios, and, obviously, these bodies do not really understand each other due to different terminologies and ontologies at different layers of the stacks. This will be up to the most innovative mobile operators to create a special consortium for each vertical (driving, health, energy, and so on) with the corresponding vertical industries. China Mobile has set up four verticals with a dedicated company for each one to look at the entire scenario and do massive trials.

As a case in point, for instance, in Kuwait, the main mobile operator ZAIN is one of the first 5G deployers, as the spectrum was given free of charge to its mobile operators, and ZAIN has created a company to use drones to control the oil fields. It's worth a couple million dollars.

These verticals will be, for sure, the biggest topics in this decade for cybersecurity, though industry might get it right but could hide their issues like anyone else.

McGRAW: MLsec is far more involved than adversarial images. ML systems are riddled with risks. At the Berryville Institute of Machine Learning, we have identified 78 risks that should be carefully considered and mitigated when engineering is building and deploying ML. ML is used for far more than simply autonomous systems, for what it's worth.

POTTER: I think we're still a long way from autonomous systems being part of our daily lives due to overt threats, like adversarial images, and inadvertent threats, like "reality is more complicated than a lab environment." In closed environments, I think we can remove the human element pretty easily. But in open-world environments, we're still miles away from being able to let these systems run free. Once adversarial images aren't a concern (that is, the technology is good enough to recognize the difference between a pineapple and an owl, or a piece of electrical tape doesn't change a 35 mi/h zone into an 85 mi/h zone), then we can have autonomous systems everywhere.

VIEGA: For image processing, if I want to break onto your phone, I can still use a passcode, hold the phone up to your face, or use a zero-day to just break onto the phone. These options are generally easier, and we can expect people to follow the path of least resistance. That's a testament to the quality of Face ID for raising the bar.

Beyond authentication, I haven't seen ML techniques provide the most effective lines of defense. If they did, then I'm sure adversarial learning would have more of a real-world impact. In general, the industry is heavily leveraging algorithms, but without enough regard to the quality of the inputs to those algorithms.

***COMPUTER*:** Governments and corporations provide extensive advice on cybersecurity. Are average users becoming more aware of cyberthreats and of how to protect themselves? Are they following the security experts' advice?

BRICKEY: Average users are becoming more aware, but it's difficult for people to keep pace with changes in technology. Unfortunately, as more and more people experience a cyberattack of some sort, they are getting more familiar with the concept. Groups like the AARP, Security Advisor Alliance, and a number of other organizations (such as the Global Cybersecurity Alliance) are spreading the word to increase awareness; however, the attack surface is increasing quicker than our ability to train people at scale.

GARFINKEL: These are questions of fact that need to be answered with research. For example, a 2019 survey of about 4,800 participants by InternetNZ found that 10% of respondents were "a little or not at all concerned about security," a finding that the authors found "worrisome."[2] A U.S. survey of 2,000 students at a large public university and its branch campuses located in the U.S. Pacific Northwest garnered a 24.9% response rate and found that 57% had personally experienced a cyberthreat, 77% have antivirus software installed on their computer, 55% had made an online purchase while logged onto a public Wi-Fi network, and 37% had shared their passwords with another person. Perhaps most significantly, "32% of students agreed that the steps needed to protect their online security and privacy is too overwhelming to think about."[3]

So, some people are following expert advice, and others aren't. Ideally, we would build systems that make following advice less important. Experts should also offer better advice. For example, there should be no security risk when using a modern web browser on a public Wi-Fi network.

LADID: Computer emergency response teams (CERTs) do an excellent job. However, looking at the cybersecurity map (https://globalsecuritymap.com/), I am not sure CERTs are efficient in their tasks.

There is a huge lack of skilled cybersecurity experts, even of security experts. Security is a very expensive investment with no immediate return on investment; hence, it is delayed or left until a disaster happens, and then the chief executive officer understands its value, but then he or she will still see it as a penalty.

McGRAW: No. Users remain blithely ignorant, and too much generic computer security advice is inconsistent and even incorrect.

POTTER: Eh. I think people continue to think about cybersecurity wrong, and that's OK. Properly designed systems shouldn't require experts' advice to be used securely. They should just work that way. Plus, people overpersonalize threats and believe that at every Starbucks there's a criminal trying to steal their credit card and that every public charging cable is trying to hijack their phone. In reality, *these threats don't even exist*, but it's top of mind for many consumers. They've heard messages about wireless snooping and plug jacking and think it's happening everywhere. It's actually happening nowhere. So, let users do their thing, and let's build them more secure systems.

VIEGA: No—should we expect them to? I think the security industry is in a bubble, and it expects security to be at the top of every company's and every person's priority list. Often, it's so far down the list that it takes regulatory compliance to drive significant spending.

As for users, if they live their lives in so much fear that they worry about cyberthreats day to day, then the industry on the whole has failed them because almost nobody wants to live that way.

***COMPUTER*:** Does cybersecurity guidance generally keep pace with new threats, or if not, to what degree does it lag?

BRICKEY: I would say it lags significantly. Larger companies and governments do a pretty good job of keeping pace, but the smaller the enterprise, the less likely that it can keep up.

GARFINKEL: In my experience, cybersecurity guidance keeps pace with new threats but not with cybersecurity research. For example, many organizations that received guidance were fast to install software patches against the Meltdown and Spectre side-channel vulnerabilities, but those same organizations have not revised their policies to allow password managers or remove the requirement for quarterly password changes. Another example: NIST 800-63B, "Digital Identity Guidelines," revised June 2017, states, "Verifiers SHOULD permit claimants to use 'paste' functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used, and in many cases, increases the likelihood that users will choose stronger memorized secrets." Nevertheless, many financial and government websites disable the paste button on critical forms.

LADID: The one who has the skills is first, and, obviously, it's on the side of the attacker. New AI-based cybersecurity simulate attacks on the networks to constantly fix the holes in the networks and predict the attacks. Investing in prevention, similar to emergency and safety services, is a way forward. But we do not have too many security software companies with worldwide span, apart from one or two.

McGRAW: Depends on who we're talking about. If we want to make a dent in the security problem, we need to focus on educating and informing engineers and operators of advanced systems.

POTTER: For enterprises, I think guidance for the secure use of systems really comes in waves. As new technology is developed, we deploy first and then think about security later. Look at Kubernetes as an example. There are a lot of companies moving to Kubernetes, but there's nearly zero accepted guidance on how to do it securely. Most companies are figuring it out as they go and are trying to put in appropriate controls. But we're a long way from where (for example) we are with enterprise endpoints. You want to know how to securely deploy and operate laptops? W00T! There are mature products, a huge body of knowledge, and lots of good processes. Technologies like Kubernetes will get there eventually, but security guidance will always lag.

> Generally, the industry is incredibly reactive, always being asked to secure the projects and technologies other people already ramped up.

VIEGA: Generally, the industry is incredibly reactive, always being asked to secure the projects and technologies other people already ramped up. It also doesn't help that the industry was originally stocked with network people, and the world is much more software driven. I'd say the security industry is generally three to five years behind the rest of the tech industry, and I don't see that changing quickly.

***COMPUTER*:** Cyberthreats arise from the vast amount of consumer data collected and stored, an attractive target for cybercriminals and other malicious actors. But new privacy laws, such as the EU's GDPR, give the public more control over their data. How will evolving privacy rules affect the cybersecurity landscape?

BRICKEY: They should help consumers with their data, but they won't help security much. The only benefit for consumers is that companies will be held financially liable with these new laws, but it will increase the cost of doing business, and that will be passed to the consumers.

GARFINKEL: Some new privacy laws come with heavy fines and statutory damages for the misuse of consumer data or for data breaches that result from data-handling practices that are inconsistent with industry standard practices. Such laws may cause companies to take cybersecurity more seriously. However, these laws may also have the perverse side effect of encouraging hackers to break into corporate data banks so that the companies can be extorted.

Overall, it's important for security professionals to remember that the main purpose of these privacy laws is to restrict what authorized users can do with the data that they already have in their possession. As such, I expect these laws to stimulate interest in access controls and auditing—two areas that have not received much attention in recent years.

LADID: Not sure GDPR is resolving any problem; on the contrary, it is now overabused by even serious websites to get people to sign off on the cookies to have access. That was not the intended purpose of this bureaucratic idea. Don't get lawyers involved in technologies they don't understand; there are a thousand loopholes.

McGRAW: They won't matter much at all, sadly.

POTTER: I think as these laws spread around the world, the impact will be profound. Companies have largely been able to do anything they want with personal data, assuming they keep them secured. Users are starting to have a say, and it's going to require companies to have much better operational control than they've had in the past. For instance, requesting a company to delete all their data about me is likely a very manual process for most U.S.-based companies. Once this right is codified into law, companies will have to make investments in automating that process. The side benefit is that they will centralize data and get better control over it, which will lead to better hygiene and security in general.

VIEGA: It will drive more spending, but in a way that continues to put an oversized burden on development organizations. I think the world can absorb it and benefit from somewhat better control over their data and somewhat less risk. But I haven't seen enough evidence yet to say for sure.

***COMPUTER*:** Are there any promising new security or privacy paradigms for addressing cybersecurity threats?

BRICKEY: The most promising aspect of cybersecurity is developing a better workforce and training them to solve problems and think like our adversaries. No specific tool is going to help, but our workforce—armed with good technology and processes—can go a long way.

GARFINKEL: Two technologies that we have been exploring at the U.S. Census Bureau are differential privacy and secure multiparty computation. Both of these offer new approaches for protecting the privacy of confidential information about individuals while allowing that information to be used in a way that benefits the public good. These technologies have rapidly matured in recent years and are now ready to be deployed at scale to solve a wide number of problems.

LADID: The vendors (all industries and their shops) are exploiting privacy to get their customers to buy more of their stuff. Go to a marketing conference and talk about respecting privacy, you will be looked at as communist against the cherished capitalism. I had that experience, so I now avoid marketing conferences.

McGRAW: We need to focus some of our existing ideas around architectural risk analysis on ML.

POTTER: I think the time for formal methods may finally be at hand. The work that Google and others are doing on formal methods is showing promise of working at a scale we haven't seen yet. Combined with the push toward more SaaS offerings, this means that code will be more centralized when compared to code in legacy enterprises. It means we may finally have a chance of verifying code and helping protect a large number of people with a small tech investment.

VIEGA: In terms of tackling the biggest problems we have, such as our social media problem, I don't see any technology emerging over the next few years that I expect will be a magic wand, if that's the question.

Security is like the nuclear arms race—there's a feedback loop pushing both the defenders and attackers to get better. Things are generally improving, and as an industry we've made some huge improvements that are worth celebrating. But a definitive solution to any one problem just shifts the playing field; it doesn't stop the game.

There are several takeaways from this VRT, one of them being that, by the year 2025, one of the leading types of cyberthreats will be the misappropriation and use of data to inflict geopolitical instability. The disturbances attackers can effect will become increasingly amplified as society becomes ever more dependent on being always connected through the cyberphysical systems that comprise the IoT. These disturbances may be further amplified by the rapid adoption of ML and higher levels of machine intelligence into the full gamut of systems upon which society relies for peace and stability.

Another takeaway is that the cat-and-mouse game between the defender and attacker will continue to be asymmetric; that is, the maxim will continue to hold that the effort expended by the defender is much greater than that of the attacker. DevOps, as practiced in 2025, could play into the hands of attackers unless the security community shores up the protection of our software-development processes. In addition, the prevailing view among the participants in this roundtable is that software quality will continue to be poor in terms of reliability and security. There is hope that developers will adopt good security and software engineering practices, such as formal methods and secure programming languages, but the view is that economics, not legislation or policy, will drive software quality.

A third takeaway is that the complexity of cybersystems and the information infrastructure on which they operate will continue to grow, with guidance on security and privacy practices continuing to lag well behind the adoption of new information technology. Furthermore, as with today, in the year 2025, users cannot be expected to understand the detailed technical aspects of the risks that cybersystems and information infrastructure pose to them. However, security and privacy experts will need to do a better job of hardening systems and infrastructure, making them wear their security and privacy policies on their sleeves. We thank the participants of this VRT for giving us insight into the set of cyberthreats and attendant challenges we can expect to encounter in the year 2025. C

DISCLAIMER

The views and conclusions contained herein are those of the panelists and authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of their employers. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes, notwithstanding any copyright annotations thereon. Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

REFERENCES

1. L. Ladid and J. Armin, "White-paper: The Finnish electronic communications regulator TRAFICOM—A cybersecurity reference model for Europe," European Union Systemic Analyser in Network Threads Consortium, Athens, Greece, White Paper, Feb. 2019. [Online]. Available: https://project-saint.eu/sites/default/files/whitepaper_1_ul_cybe_final_1.pdf
2. S. S. Tirumala, M. R. Valluri, and G. Babu, "A survey on cybersecurity awareness concerns, practices and conceptual measures," in *Proc. 2019 Int. Conf. Computer Communication and Informatics (ICCCI)*, Coimbatore, India, pp. 1–6. doi: 10.1109/ICCCI.2019.8821951. [Online]. Available: https://ieeexplore.ieee.org/document/8821951
3. D. Sarathchandra, K. Haltinner, and N. Lichtenberg, "College students' cybersecurity risk perceptions, awareness, and practices," in *Proc. 2016 Cybersecurity Symp. (CYBERSEC)*, Coeur d'Alene, ID, pp. 68–73. doi: 10.1109/CYBERSEC.2016.018. [Online]. Available: https://ieeexplore.ieee.org/document/7942427

JAMES BRET MICHAEL is a professor in the Naval Postgraduate School's Computer Science and Electrical and Computer Engineering departments. Contact him at bmichael@nps.edu.

RICHARD KUHN is a computer scientist in the Computer Security Division at the National Institute of Standards. Contact him at kuhn@nist.gov.

JEFFREY VOAS is the editor in chief of *Computer*. Contact him at j.voas@ieee.org.