Computing Community Consortium (CCC) Response to NITRD
"RFI on Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan"

Nadya Bliss, Ann W. Drobnis, Kevin Fu, Daniel Lopresti, Keith Marzullo

This response was prepared by the Computing Community Consortium (CCC). The mission of the CCC is to catalyze the computing research community and enable the pursuit of innovative, high-impact research. Our goal is to identify and call attention to major research opportunities for the computing community.

The Federal Cybersecurity R&D Strategic Plan outlines the continued need for basic research in Cybersecurity, a focus that is crucial for our continued leadership in the area. However, the current plan is more than two years old, and this is a field that is moving very quickly. We are pleased that the NITRD NCO and the Select Committee intend to update the Strategic Plan to reflect current priorities.

The Request for Information asked six questions. Given the community workshops and reports we have held on related topics over the past year, and on the future events to be held by the CCC, we focus on Questions 3, 4 and 5. An overarching question, however, is: what does *cybersecurity* mean now? A traditional definition (from Kapersky Labs, US) is:

> Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
> *https://usa.kaspersky.com/resource-center/definitions/what-is-cyber-security*

Such systems and devices used to be the purview of experts, but are now ubiquitous: they are widely used by individuals, organizations, and societies for activities ranging from social to life-critical. The information and communications technology (ICT) that needs defending are components of socio-technical systems: the involved people are integral parts of the systems as well. Thus, it is increasingly important to think of how to defend the people, organizations, and societies from malicious attack as well as the ICT. Indeed, many of the malicious attacks (that is, attacks that are meant to do harm) are social in nature, ranging from phishing attacks to

nation-state led acts of disinformation. As such, it is time for the community to consider adjusting our definition of what constitutes cybersecurity by explicitly adding the people who use and are affected by the computing and communications systems to the ecosystem that requires protection. By doing so, problems that have not traditionally been considered cybersecurity in nature – cyber-bullying, cyber-crime, and the use of ICT in supporting human slavery – are important to include when scoping the R&D agenda of cybersecurity.

3. What areas of research or topics of the 2016 Strategic Plan should continue to be a priority for federally funded research and require continued Federal R&D investments?

We identify three areas that should continue to be a priority.

1. The report calls out the human aspects of cybersecurity as a critical dependency. This remains critical. The CCC recently held two workshops on socio-technical issues in cybersecurity, and many of the research areas identified in the report emerged in the workshops as being important. Other research questions emerged, such as: How can organizational structure and practice incentivize the design of secure systems? What are ways to approach the tension between the desire of law enforcement to be able to access data in individual's devices and the desire of corporations who design these devices to provide products that meet market needs? Which practices and organizations can be set up or adapted to collect the cyber-crime data needed to enable impactful cyber-criminology research and practice? More interdisciplinary efforts are required to address such questions, which are only going to increase in importance due to the socio-technical nature of our ICT-enabled infrastructure.

   A stumbling block in this work is the difficulty of conducting interdisciplinary research. The National Science Foundation has made a strong first step in enabling such efforts through its Secure and Trustworthy Computing program, but there are still barriers. Enabling and supporting interdisciplinary research (and development of associated metrics) in this area will take continued attention from both the public and private sectors.

2. The Internet of Things (IoT) and Cyber-Physical Systems (CPS) were called out in the plan as disruptive technologies that are increasingly important. Some of the problems arise from the sheer scale of such systems, which Statistica predicts will soon exceed 30 billion connected devices worldwide - and support over 60 billion such devices within five years. Also called out in the report is Cloud Computing because of its widespread adoption over the last decade. Over the last three years, however, edge computing (or fog computing) has emerged as an important enabler with respect to IoT and CPS, since edge computing will provide the computational layer that supports many of the IoT and CPS applications. Underlying this ecosystem is the rapidly developing 5G wireless

technology as well as the more established software defined networking/software defined infrastructure, all of which are complex systems with new attack surfaces.

This convolution of technologies and infrastructure requires a more holistic approach to cybersecurity for IoT and CPS, as well as more coordinated research by those developing the new technologies and those developing the underlying infrastructures. These efforts should also include development of consistent security standards and benchmarks across diversity of technologies. Doing this is hard due to the sheer scale of technologies and interests. This kind of approach can be best supported by partnerships among Federal labs and agencies, the private sector, and universities. The Federal government has the best leverage for making such partnerships a reality.

3. Finally, the plan called for research into long-term confidentiality, such as quantum-resistant cryptography. Advances in quantum information systems are being steadily made, and both its use and its defense in terms of cybersecurity require continued research. In a recent CCC workshop on quantum computing, it was noted that while QC implementations sufficient to break public key cryptography on practical key sizes are still many years away, research is needed in advance of that day towards "post-quantum" public-key cryptographic systems that can resist quantum attack and maintain security. The CCC is holding a second workshop on this very topic - Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility[1] - in February, 2019, with a community report from the workshop to follow.

   Some of the leading candidates for such post-quantum systems are based on lattices: no efficient quantum algorithms are known yet for breaking such cryptosystems. However, the main way that we gain confidence in the security of a cryptosystem is by attacking it. Thus there is an urgent need to study possible quantum algorithms for lattice-based cryptosystems (as well as code-based cryptosystems) to determine whether these, too, will turn out to be vulnerable. And, since cryptosystems are foundational and are slow to replace in practice, it is important to know whether an algorithm for breaking lattice cryptosystems will be possible long before the algorithms are implemented.

4. What challenges or objectives not included in the 2016 Strategic Plan should be strategic priorities for federally funded R&D in cybersecurity? Discuss what new capabilities would be desired, what objectives should guide such research, and why those capabilities and objectives should be strategic priorities.

Despite it being less than three years since the last plan was released, there are vulnerabilities that have become evident since the release of the current strategic plan.

---

[1]https://cra.org/ccc/events/identifying-research-challenges-in-pqc-migration-and-cryptographic-agility/#overview

One key vulnerability that has become prominent recently is the ability to rapidly spread misinformation and disinformation throughout computing systems with the specific goals ranging from manipulating opinion to leading to destructive actions (including inciting riots, as has happened in India, to potential interference in the election process, including the recent Brazilian presidential election). This is a strategic research priority that is much broader than the United States and would benefit from international collaboration. The confluence of the broad reach of social networks at very large scales and non-technical fields such as narrative influence, psychology, public policy, journalism, and political science need to be brought together and supported by further research investment.

This is only made harder by the falling trust people have worldwide in their public and private institutions. The annual Edelman Trust Barometer surveys tens of thousands of people across 28 countries about four institutions: business, media, government, and NGOs. Their 2017 survey reported a decline of trust in all four institutions for the first time since the survey began in 2001. They reported that government was the least trusted institution, and media, taking its biggest ever year-on-year hit, is now distrusted in 82% of the countries that were surveyed. Their 2018 report shows little change from 2017, with one notable exception: in the United States, the percent trust by the informed public over all four institutions dropped between 20 to 30 points: worldwide, the United States fell from sixth to last place (among the general population, the U.S. fell from eighth to 18th place worldwide). In circumstances like this, even the source of funding can be weaponized: indeed, it has been. International efforts could help alleviate this loss of trust, as well as by increasing partnerships with private foundations.

A related area that is emerging as a broad vulnerability is tampering with images and video data, an example being deepfake. The rapid increase in ability to construct such visual information, and the use of algorithms to continuously increase the difficulty of detection, has the possibility of accelerating the decrease in trust in public and private institutions. Broadly, techniques for identifying fake data and its origin in diversity of modalities are needed as well as finding ways to help people identify ways to build trust in the face of untrustworthy information sources.

Similarly, the notion of ‘hacking’ machine learning algorithms (particularly in the context of classification and recognition) is another area that has recently received increased attention and requires further investment.

The use of algorithms and machine learning (ML) is having a large (and for the most part, very positive) impact on our economy and society. Advances in artificial intelligence (AI) will provide opportunities for increased automation on protection of cyber physical and other socio-technical systems. But, using AI also increases the potential attack surface, expanding the opportunities for attacks at algorithmic level. It is now a priority to address how to protect ML and AI from attacks such as manipulating training sets and using the same sets to train attack software. As

above, this is another area where investment is necessary both in core computer science research (essentially identification of algorithmic vulnerabilities) and in interdisciplinary research.

This last point is worth further elaboration. The report's fourth recommendation was to *expand the diversity of expertise in the cybersecurity research community.* Quoting the report,

> Cybersecurity needs extend beyond technology, requiring deep understanding of the human facets of cyber threats and secure cyber systems. To accelerate progress, the skills of traditional cybersecurity researchers should be augmented with expertise from social, behavioral, and economic disciplines.
>
> Multi-disciplinary research should be promoted by funding agencies and by research institutions. Agencies should ensure that grant solicitations and grant review processes are open to multi-disciplinary proposals. Research institutions should ensure that advancement (e.g., tenure) decisions value multi- disciplinary research successes and publication in nontraditional journals and conferences equally with traditional tenure criteria.

While this is still an excellent recommendation, the need for interdisciplinarity extends past the need for deep understanding of the human facets of cyber threats and secure cyber systems. Cybersecurity in the context of the emergence of cryptocurrencies requires an understanding of economics, and cybersecurity in the context of electronic health records requires understanding in privacy, health law, and operations research. Such a broad diversity is not easily supported by a single Federal agency. Agencies such as the Department of Justice, the National Institutes of Medicine, the Department of Transportation – that is, agencies that support research grants and whose mission includes verticals that intersect with cybersecurity – should partner in programs like NSF's Secure and Trustworthy Cyberspace as a way to expand the diversity of the cybersecurity research community.

5. What changes to cybersecurity education and workforce development, at all levels of education, should be considered to prepare students, faculty, and the workforce in the next decade for emerging cybersecurity challenges, such as the implications of artificial intelligence, quantum computing, and the Internet of Things on cybersecurity?

Although it remains vital, cybersecurity education and workforce development must be more broad than what is covered in Computer Science programs. For example, there is a great need for educating the workforce on the basics of secure design, and how to apply standard guidelines and frameworks to the building of secure products and systems. Similarly, it is necessary to educate developers on the use of privacy-by design techniques to guarantee that both security and privacy safety measures are built into products from their onset. As we have painfully learned, retrofitting privacy and security is destined for failure.

Users of products would also benefit from general security and privacy education campaigns aimed at making them aware about simple secure configuration options for home devices, typical scams performed via email or social media, the perils of sharing too much information, and practicing simple cyber-hygiene, all of which can go a long way towards protecting their personal information. Such approaches are already being actively deployed in companies with the aim to minimize security incidents. It is obvious that the general population would benefit from such approaches as well.

Cybersecurity education for policy makers and corporate executives is of growing importance. Such programs resemble, in some ways, programs for the general public: they can not require a strong technical background. But, they would need to focus more on assessing and calculating risk, and on the legal framework around cybersecurity.

The demand for such education is growing quite rapidly, and is being met in part by non-traditional education programs. This is, of course, a positive development: the problem is broad enough that non-traditional delivery should be explored. Unfortunately, much of what is currently offered are tool-based programs: they teach people how to use tools rather than teaching them the fundamentals, and have low rigor. It would be worthwhile to explore ways to encourage such educational programs to have a syllabus that conforms with the NIST Cybersecurity Framework.

Finally, the need for a strong cybersecurity workforce requires an “all-hands-on-deck” approach. Our programs and degrees must be inclusive of women and underrepresented groups. We must continue our efforts to increase diversity and inclusion in cybersecurity education. The problems are too wide-reaching, and the impacts too severe, for us to exclude promising young people, even if only due to oversight or inertia.

APPENDIX

The following is a list of CCC workshops (associated community reports can be found at the link) that have discussed issues which intersect the issues raised by the RFI.

Security

- Sociotechnical cybersecurity: https://cra.org/ccc/visioning/visioning-activities/2016-activities/sociotechnical-cybersecurity/
- Cybersecurity for Manufacturers: https://cra.org/ccc/events/cyber-physical-security-manufacturers-workshop/
- Leadership in Embedded Security: https://cra.org/ccc/events/embedded-security-workshop/

Artificial Intelligence

- AI for Social Good: https://cra.org/ccc/events/symposium-ai-social-good/
- AAAI Symposium on AI for Social Good: https://cra.org/ccc/events/symposium-ai-social-good/
- Symposium on Accelerating Science: A Grand Challenge for AI: https://cra.org/ccc/events/symposium-accelerating-science-grand-challenge-ai/

Smart Health/IoT

- Discovery and Innovation in Smart and Pervasive Health: https://cra.org/ccc/events/discovery-innovation-smart-health/
- Sociotechnical Interventions for Health Disparity Reduction: https://cra.org/ccc/events/sociotechnical-interventions-health-disparity-reduction/

Quantum Computing

- Next Steps in Quantum Computing: https://cra.org/ccc/events/quantum-computing/

Education

- Computer Aided Personalized Education: https://cra.org/ccc/events/computer-aided-personalized-education/

The following is a list of CCC white papers that have discussed issues which intersect the issues raised by the RFI.

Security

- Enabling Advanced Intelligence and Decision Making for America's Security: https://cra.org/ccc/wp-content/uploads/sites/2/2015/05/Intelligence.pdf

Artificial Intelligence

- Toward a Science of Autonomy: Defense: https://cra.org/ccc/wp-content/uploads/sites/2/2015/01/Defense-v4.pdf

Smart Health/IoT

- Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things: https://cra.org/ccc/wp-content/uploads/sites/2/2017/02/Safety-Security-and-Privacy-Threats-in-IoT.pdf
- Safety and Security for Intelligent Infrastructure: https://cra.org/ccc/wp-content/uploads/sites/2/2017/03/Safety-and-Security-for-Intelligent-Infrastructure.pdf

Education

- The Importance of Computing Education Research: https://cra.org/ccc/wp-content/uploads/sites/2/2015/01/CSEdResearchWhitePaper2016.pdf