Andrea Little Limbago
Endgame

"Input to the Commission on Enhancing National Cybersecurity"

Executive Summary
Topic Area: Cybersecurity Research and Development

Challenges:

The industry is long overdue for game-changing innovation, but remains too insularly focused to truly provide the paradigm shift so badly needed. This paradigm shift is not purely a technological one, but requires cross-disciplinary R&D efforts and a shift in mindset to achieve game-changing results. In some cases, such as AI and hunt, a cultural shift and new mindset is required. However, in many cases the infrastructure may not support the newest R&D developments, and therefore additional incentives may be required to achieve greater security. Implementation and operationalization is one of the biggest challenges and is factored into all of these recommendations.

Recommendations:

To cover the broad spectrum of technological and human-based vulnerabilities, current and future R&D should explore: 1) the purely technological basic research; 2) human-computer interaction (HCI); 3) quantitative and computational social science models. Together, these require a shift in mindset, assuming organizations have been breached, and moving toward learning systems that adapt to both the internal and external threat environments. The following recommendations cross each of these three areas for a holistic R&D portfolio across the industry.

- **Artificial Intelligence & the Hunt:** We are in the early stages of understanding the efficacy of the mentality of assuming breach and pursuing a hunt approach. This R&D should further move the industry toward completely eliminating the detection gap instead of accepting days or even months of dwell time. Artificial intelligence capabilities – such as unsupervised machine learning approaches, including user and entity behavior analytics – should go hand in hand with research embedded within a hunt framework to automate the search, detection and eviction of the adversary, while automating many of the processes that remain overly manual and time and resource intense. As occurs in the tit-for-tat world of adversarial behavior, AI should also inform adversarial models to prevent classes of exploits and vulnerabilities, building on multi-player game theoretic models of one defender against multiple adversaries.
- **Tackling Disinformation:** While most big data analytics has focused on the volume, variety, and velocity of the data, the veracity of data remains a largely underexplored area, and yet may have an enormous impact. Altered data has the ability to impact both the political and economic systems, especially if the public begins to question the veracity of key data – such as financial data or election results.
- **Policy Innovation:** There is a desperate need to define acceptable behavior in the digital domain, while simultaneously enhancing deterrence capabilities. Computational social science models – including quantitative, formal, and agent-based models – should explore the unique challenges and optimal policies for norm diffusion and deterrence.

Andrea Little Limbago
Endgame
"Input to the Commission on Enhancing National Cybersecurity"

Comments: Cybersecurity Research and Development

Public and private sector organizations are devoting significant resources toward cybersecurity research and development (R&D). However, as breach after breach occurs, it's clear that there are systemic hurdles that limit the ROI on those R&D investments. The industry is long overdue for game-changing innovation, but remains too insularly focused to provide the paradigm shift so badly needed. This paradigm shift is not purely a technological one, but requires cross-disciplinary R&D efforts and a shift in mindset to achieve game-changing results.

The majority of applied R&D cybersecurity solutions have stumbled into the trap of focusing on solving yesterday's problem without looking ahead to explore what the next great challenge may be. Furthermore, the old adage of old wine in new bottle is unfortunately quite fitting to the current state of cybersecurity, including many of the R&D efforts that continue to focus on signatures or assuming closed systems. Unlike many other technology-based fields, cybersecurity has yet to truly embrace or leverage many of the advances made in other sciences. This has left the industry in the current reactionary state that is neither sustainable nor desirable. To cover the broad spectrum of technological and human-based vulnerabilities, current and future R&D should explore: 1) the purely technological basic research; 2) human-computer interaction (HCI); 3) quantitative and computational social science models. Together, these require a shift in mindset, assuming organizations have been breached, and moving toward learning systems that adapt to both the internal and external threat environments. The following recommendations cross each of these three areas for a holistic R&D portfolio.

Artificial Intelligence and the Hunt

First, artificial intelligence (AI) possesses the most obvious potential for radically disrupting the industry. Given both the customization of malware, as well as the dynamic adversarial command and control infrastructure, cybersecurity defenses should explore new technologies that turn them into learning systems. Unsupervised machine learning approaches – such as those focused on user and entity behavior analytics – works at the intersection of human behavior and big data analytics. Future solutions should focus on removing the human from the loop as much as possible. This is where the learning aspect is essential and can help increasingly minimize false positives. To be clear, this does not imply automated strategic decisions, but more so the automation and evolution of protection and detection, while minimizing false positives. Instead of viewing defenses as static protections around finite entities, cybersecurity should be viewed as a learning system that evolves with additional data, reflecting a system-within-systems environment, each of which also exhibit micro-environments that can inform anomalous behavior at various levels within the system.

As occurs in the tit-for-tat world of adversarial behavior, AI should also inform adversarial models to prevent entire classes of exploits and vulnerabilities. This evolves beyond the reactionary responses as each new vulnerability is identified, and progresses to prevent even those unknown behaviors. This is also where game theoretic models can

inform the AI parameters. Both the adversary and the defenders will need to be increasingly adaptable, while multi-player game theoretic models can inform the parameters of any AI model with one defender against multiple adversaries.

AI-focused R&D is integral to detection and prevention, but it is unlikely to be 100% effective. Therefore, the next area for focused, applied research should continue to explore the best and most effective means to hunt within networks in real-time. As offensive capabilities continue to evolve in sophistication, these same techniques can be employed for hunting the adversary within networks. We are in the early stages of understanding just how effective a hunt approach can be. R&D in this area should further move the industry toward completely eliminating the detection gap instead of accepting days or even months of dwell time. The AI capabilities should go hand in hand with research embedded within a hunt framework to automate the search, detection and eviction of the adversary, while automating many of the processes that remain overly manual and time and resource intense. Looking ahead toward longer term basic research, R&D should explore the integration of hunting methodologies with alternative interfaces and command and control mechanisms, leveraging much of the virtual reality and gaming technologies that could reflect the interfaces of the future.

Tackling Disinformation

Historically, when data was digitally stolen, it remained hidden or concealed by the attacker. Increasingly, this data is just as likely to be publicly released, containing a combination of valid and altered data that maximizes the desired impact. While most big data analytics has focused on the volume, variety, and velocity of the data, the veracity of data remains a largely underexplored area, and yet may have an enormous impact. This is well worth the research investment, as altered data has the ability to impact both the political and economic systems, especially if the public begins to question the veracity of key data – such as financial data or election results.

Similarly, bots are increasingly employed to spread disinformation, especially on social media. R&D efforts to distinguish between content created by bots and humans could be beneficial to tackle the rising use of disinformation. This could include the use of natural language processing aimed at the content itself, or analytics on time frequency and other temporal patterns to expose the bot-driven behavior. Given that bots are an increasing percentage of web traffic, any capability must also be able to separate disinformation from the streams of 'legitimate' bot-driven advertising. This obviously becomes much more nuanced, and would in turn require large-scale correlation against similar information, but dissimilar data structures, on the web.

Policy Innovation

Policy innovation is not traditionally associated with R&D, but due to improved computational social science techniques over the last decade, it would be well worth the investment. Given the lasting influence of these policies, it also absolutely requires technical input to ensure the next series of policies prepare the US for the anticipated threat and technological landscape for decades to come. The first focal area should

address altering the incentive structure to encourage individuals and organizations to implement the 'low-hanging fruit' of basic cyber hygiene and stopping many of these preventable breaches that occur today. Failing to get the 'easy' solutions implemented limits the potential for implementation of the more difficult and sophisticated future efforts. This effort would evaluate economic, cultural, and institutional incentive models to identify the most optimal policies that would lead to wide scale adoption of cybersecurity best practices. This focal area should include short-term solutions to address the need for manual patching, while also pursuing an optimal solution to automate patches, incentivizing tech companies to bake automated updates into products as a longer-term approach, as well as how to incentivize organizations to employ the solutions that exist today.

Additionally, there is a desperate need to define acceptable behavior in the digital domain, while simultaneously enhancing deterrence capabilities. Unfortunately, norm diffusion is a significant challenge. Norm diffusion in cybersecurity is unlikely to reflect many previous norm diffusion models. It would be worthwhile to formulate a range of norm diffusion models that identify the best approach to increase the probability of the greatest norm diffusion, taking into consideration the unique nature of the cyber domain, including collective action problems, attribution challenges, rational choice and cultural relativism, among other social considerations. In contrast, we should not assume that norm diffusion would succeed, and it certainly will not in the near future. Therefore, it should be coupled with greater research into deterrence and specifically how to best formulate a credible, cross-domain deterrence capability in a world where attribution and intent are both difficult to ascertain. For instance, can offensive capabilities be exposed to increase deterrence or must they remain concealed? To say our understanding of digital deterrence – and how it fits into cross-domain solutions – is nascent is a vast understatement. As many scholars have noted, we're decades behind where we should be in this realm, and it is further contributing to the current offensive free-for-all that is only going to grow, as corporations increasingly demand greater offensive capabilities. In each of these areas, computational social models, including formal, quantitative, and agent-based models, could all help greatly inform leaders and encourage the policy modernization desperately needed.

Future Challenges

Implementation and operationalization is one of the biggest challenges for any of these recommendations. In some cases, such as AI and hunt, a cultural shift and new mindset is required. Even with those changes, in many cases the infrastructure may not support the newest R&D developments, and therefore additional incentives may be required to achieve greater security. Finally, future-leaning R&D should focus on moving the needle toward the creation of learning systems, which take into account both the technical anomalies as well as those driven by human behavior. It is certain that the cat and mouse game will continue, and the US will require innovative learning defenses, modernized and scientifically driven policies, and a means to extrapolate data veracity from the noise.

Andrea Little Limbago
Endgame
"Input to the Commission on Enhancing National Cybersecurity"

Executive Summary
Topic Area: Cybersecurity Workforce

Challenges:

The well-publicized skills gap, pipeline shortage, and lack of diversity combine to make the cyber workforce one of the most challenging recruiting markets for employers. Unfortunately, across the board, the situation only seems to be worsening. The anticipated supply of skilled workers will not meet the projected demand, a gap that is only likely to grow over the next decade. Simultaneously, retention of the current skilled security workforce is also a serious but underexplored issue, as many leave due to burnout or an antagonistic work environment. Cybersecurity faces severe cultural and public relations challenges that continue to impact retention and recruitment in the field.

Recommendations:

There must be concerted public and private sector efforts to holistically address the workforce challenges. These can loosely be grouped by the skills gap and pipeline shortage, retention, and external perception.

- **Skills Gap & Pipeline Shortage:** Identifying cross-disciplinary skillsets that are relevant for security applications can ameliorate this supply and demand incongruity. Cross-disciplinary secondary and university education programs should increasingly include a computer science core requirement, with a focus on security. Garnering interest as early as elementary school should also be a priority, mandating computer science training, and supporting non-profit coding groups aimed at under-represented groups.
- **Retention:** Cybersecurity, as part of the tech community, must move beyond the brogrammer culture reputation and appeal to a more diverse workforce. The failure to provide an inclusive culture impacts under-represented groups in the workforce as early as internships. Cybersecurity conferences should provide a more diverse representation of speakers on panels, ensuring greater participation of under-represented groups. Organizations should look at equal compensation and promotion propensities within the cybersecurity workforce. From a cultural perspective, organizations must focus social and team-building events that appeal to a larger demographic, while also institutionalizing corporate swag that are appropriate for a wider workforce, and instituting greater workday flexibility to avoid burnout. These very simple fixes likely seem irrelevant or quaint, but these factors are often overlooked and are core components of cultural cohesion.
- **External Perception:** The industry requires a major makeover from the common perception of the industry as one dominated by anti-social young men in hoodies working in dark environments. This misrepresents the industry and is a public relations challenge the industry must acknowledge and actively counter, such as through public service announcements, more representative marketing, and visible role models from diverse demographics.

Comments: Cybersecurity Workforce

The well-publicized skills gap, pipeline shortage, and lack of diversity combine to make the cyber workforce one of the most challenging recruiting markets for employers. Unfortunately, across the board, the situation only seems to be worsening. The anticipated supply of skilled workers will not meet the projected demand, a gap that is only likely to grow over the next decade. Simultaneously, retention of the current skilled security workforce is also a serious but underexplored issue, as many leave due to burnout or an antagonistic work environment. Below are recommendations for addressing the workforce challenges of today and the future. Any workforce strategy should focus both on expanding the workforce as well as retention.

Skills Gap & Pipeline Shortage

Many believe the graduation rate in computer science will remain well below future openings. Even among those who do graduate with a computer science degree, there is no guarantee they'll pursue security. Identifying cross-disciplinary skillsets that are relevant for security applications can ameliorate this supply and demand incongruity. For instance, with the security data environment only growing in complexity and scale, data scientists or other disciplines familiar with big data challenges (e.g., physics) must become a core part of a security team, working closely with the domain experts, while augmenting capabilities and the workforce.

Similarly, cross-disciplinary secondary and university education programs should increasingly include a computer science core requirement, with a focus on security. This not only exposes all students to the discipline, but it ensures that those who pursue non-cybersecurity degrees are much more technically competent. They will then bring that competency into the workforce, helping ensure more widespread cyber hygiene and cognizance of the cybersecurity technical challenges and impact. The United States Naval Academy provides a great educational model. Not only can students graduate with a cyber operations degree, but all midshipmen must take two cybersecurity courses. This kind of cross-pollination of disciplines will be essential in the future, and can help expose cybersecurity to those who may not have considered it an option.

Of course, garnering interest as early as elementary school should also be a priority. Many schools currently do not teach anything on cyber hygiene or coding, both of which can provide early introductions into the mission and challenges in the field. This could be coordinated with keyboard class, and thus would not occur at the detriment of the more traditional core course teaching. Additionally, groups aimed at supporting under-represented groups such as Girls Who Code, CodeNow, or Code for America, should receive support for expansion beyond the current candidate pool.

Expanding the applicant pool must be a priority. The prominent strategy today is a top-down, executive mandate for greater outreach. Unfortunately, most of these efforts have little impact, as they remain insularly focused. A few areas that would greatly expand and diversify the applicant pool include organizational and product marketing of

security products that reflects a diverse workforce, private/public partnerships with many of the hacker camps and vocational schools that offer security degrees, as well greater workplace flexibility. With technology continuing to enhance productivity away from the office, cybersecurity as an industry should embrace a greater, flexible workday for multi-generational and cross-demographic appeal. Finally, job openings should ensure they are inclusive, refraining from specific personal pronouns, and ensuring they do not rely on jargon such as cyber warrior, which may be off-putting to potential recruits.

Retention

The pipeline challenge addresses the longer-term changes that need to be made for the future cybersecurity workforce. However, any strategy must also address the near-term, current cybersecurity workforce challenges, including altering the dominant and invalid perception of the industry as a workforce of young men in dark hoodies, as well as other cultural challenges. First, cybersecurity, as part of the tech community, must move beyond the brogrammer culture reputation and appeal to a more diverse workforce. While this is a recruitment challenge as well, it is a key driver that pushes personnel away from the industry.

Additionally, cybersecurity occupies the space at the intersection of technology and national security, another male dominated field, both of which tend to be shaped by male preferences and priorities. This has led to a culture where many women and other under-represented groups experience 'death by a thousand cuts', including anything from attending conferences that may have misogynistic overtures, to being passed over for promotions, to harassment. For those under-represented groups, despite the strong desire to support the mission, a toxic environment may push many to leave the industry, as we've seen with the declining numbers of women in security and computer science. In fact, a recent study finally dispels the belief that women leave engineering due to work/life balance. Instead, it's the lack of feeling valued, limited career trajectories, and the negative work environment.

Fortunately, there are many steps the industry can take to address retention in ways that benefit the entire workforce. Within the community, both private and public sector cybersecurity conferences should provide a more diverse representation of speakers on panels, ensuring greater participation of under-represented groups, and moving beyond the tendency toward manels. Especially for the younger workforce, if they consistently fail to see any role models with whom they may identify, they are less likely to feel inclined to stay in the industry. This is true at meetups as well, as the growth and support of meetups that take a more nuanced approach to the workforce can also provide current cybersecurity personnel a place to share stories and lessons learned.

Organizations should also look at equal compensation and promotion propensities within the cybersecurity workforce, similar to Salesforce's well-publicized internal review and adjustments. This data is readily available, but most organizations are not introspective enough to see if inequities exist. From a cultural perspective, organizations

must focus social and team-building events that appeal to a larger demographic, while also institutionalizing corporate swag that are appropriate for a wider workforce. These very simple fixes likely seem irrelevant or quaint, but these factors are often overlooked and are core components of cultural cohesion. It's time for the industry to mature, while maintaining true to its roots of experimentation and innovation.

Of course, the retention challenge is not just one of fostering a more inclusive environment, but as mentioned earlier, burnout is also a growing problem in the industry. This is one area where technology can help the workforce challenge. While the industry's mission and challenges are only likely to grow, the community needs to leverage greater automation – including artificial intelligence and enhanced user interfaces. This not only can help retention, but it should provide a net positive effect on capabilities as well. The automation of rote processes especially can help alleviate the workload by enabling analysts and operators to spend more time proactively identifying anomalies and less time on manually-intensive activities such as data structuring and merging.

External Perception

Cybersecurity requires a makeover away from the common perception of the industry as one dominated by anti-social young men in hoodies working in dark environments. Not only is this a misrepresentation of the industry, but it also negatively impacts recruitment and retention across all demographics. This is a public relations challenge the industry must acknowledge and actively counter. Of course, when practically every article on the latest breach lacks the creativity to include anything other than the dark hooded figure at a keyboard, evolving beyond this perception will require an active media campaign.

For instance, public service announcements (PSA) could have the dual effect of both enhancing security and exposing the industry to a wider applicant pool. The PSAs would obviously need to reflect modern technical realities and target advertisements on social media and e-commerce sites and other popular sites that have broad demographic usage. These would not only portray the diverse demographics the industry needs, but also should emphasize the social as well as national security mission of the industry. Civic hacking, for instance, is rarely discussed, but is essential for privacy and strengthening our democratic institutions. The national security mission remains absolutely vital, but there are additional social missions that should be highlighted to reach a broader workforce. With African Americans, Hispanics, and women all represented in the single digits, the PSAs may be an important step in expanding the aperture of the industry's workforce. The PSAs should also inform the public about cyber hygiene best practices, such as including links that, when clicked, warn about adware and phishing, thereby having the additional benefit of educating the public while addressing cybersecurity's PR problem.

Final Thoughts

In sum, to ensure today and tomorrow's cybersecurity workforce is equipped to tackle the growing challenges, a variety of educational, cultural, and social approaches must be taken. There must also be greater acknowledgement at all educational levels of the biases that occur, and focus comprehensively on exposing all students to cybersecurity, similar to President Obama's emphasis on teaching all students to learn computer science. Even if the technical gap is closed, this is only a first step. At its core, the cybersecurity workforce challenge is not a technical issue, which is why so many proposed solutions have failed. The industry must adapt and return to its roots, wherein hackers are portrayed as curious and innovative, open to a broad demographic interested in working on the most complex and important challenges of modern times.