The CSIS' Recommendations on Cybersecurity for the 45th President of the United States

Victoria Yoon

Department of Information Systems
Virginia Commonwealth University

Center for Strategic and International Studies (CSIS)

- is headquartered in Washington, D.C.
- has developed solutions to the world's greatest policy challenges for last 50 years.
- has the 220 full-time staff and numerous affiliated researchers
- offers strategic insights and bipartisan solutions to assist decision-makers in developing policies.

Report of CSIS Cyber Policy Task Force

- CSIS submitted the 2009 Commission on Cybersecurity for the 44th Presidency.
- In January 2017, CSIS released a report of CSIS Cyber Policy Task Force entitled “From Awareness to Action: A Cybersecurity Agenda for the 45th President”* in January 2017. .

* Center for Strategic and International Studies, *From Awareness to Action: A Cybersecurity Agenda for the 45th President*, Task Force Chairs: Sen. Sheldon Whitehouse, Rep. Michael T. McCaul, Karen Evans, and Sameer Bhalotra, January 2017.

14 Specific Recommendations on Cybersecurity for the 45th President

1) *Modify the International Cybersecurity Strategy;*
2) *Develop a New Approach to Drawing Agreement on International Stability;*
   - Two questions:
     - Is it time to consider a more formal approach to building security and stability in cyberspace?
     - To what extent should an expanded or even continued efforts to build focus on agreement among likeminded states.
   - Two-track strategy
     - agreeing on norms with likeminded nations while pursing risk-reduction measures with the authoritarians.
3) *Extend Deterrence and Create Consequences;*
   - Recommends the threat of sanctions or indictments as the most effective deterrent actions.

14 Specific Recommendations on Cybersecurity for the 45th President

4) *Choose a More Assertive Approach to fight against Cyber Crime;*
   - To break the stalemate on the Budapest Convention,
   - penalize in some way those countries that refuse to cooperate with law enforcement.
   - find a new negotiating vehicle that preserves the benefits of the convention but gives Brazil, India, and perhaps China a new negotiation that provides them with the opportunity to take their concerns into account.

5) *Preserve Global Data Flows;*
   - need to find cooperative approaches that ensure the free, secure flow of data and, as part of rethinking international strategy.
   - require a discussion of rules (and perhaps institutions) for international cybersecurity, privacy, and digital trade.

6) *Enforce Privacy Policy for Data Protection and Privacy;*
   - start with the principle for federal programs that “data belongs to the user.”
   - build on existing efforts, including the proposal for a Consumer Data Privacy Framework and Federal Trade Commission (FTC) efforts to enforce existing privacy policies.

7) *Increased Transparency for Cyber Incidents;*

14 Specific Recommendations on Cybersecurity for President Trump

8) *Internet of Things;*
   - task NIST to collaborate with consumer and business groups to develop standards and principles for IOT security,
   - take a “sector-specific” approach to IOT security and the development of IOT resilience frameworks, and
   - use federal procurement standards to drive improvement and safeguard government functions.

9) *Encryption;*
   - task NIST to work with encryption experts, technology providers, and Internet service providers to develop standards and methods for protecting applications and data in the cloud.

10) *Active Defense;*

14 Specific Recommendations on Cybersecurity for President Trump

11) *Enhance baseline security by improving organizational governance for cybersecurity;*
   - The NIST framework was established general guidance on actions that companies can take to improve security
   - NIST should be tasked to develop the metrics to measure the adoption and effectiveness of the NIST framework.

12) *Increase the Cost to hackers;*
   - Actions to impede the monetization of stolen data and credentials.
   - Techniques to divert adversary resources toward defense and to paralyze their network infrastructure used for attacks.
   - Accelerate the move to multifactor authentication
   - Find better ways to counter and disrupt botnets

13) *Develop the close partnerships between U.S. military cyber forces and the intelligence community;*

14) *Use NETGuard, the National Guard, and the Reserves to protect critical assets in advance.*

Bright Internet* vs. CSIS Recommendations

1) Modify the International Cybersecurity Strategy

2) Develop a New Approach to Drawing Agreement on International Stability

5) Preserve Global Data Flows

BI Five Principles **CSIS Recommendations**

* Lee, J.K., Cho, D., and Lim, G.G. Design and Validation of the Bright Internet, *Journal of the Association for Information Systems*, forthcoming

Bright Internet vs. CSIS Recommendations

3) Extend Deterrence and Create Consequences

4) Choose a More Assertive Approach to fight against Cyber Crime

10) Active Defense

12) Increase the Cost to hackers

BI Five Principles

CSIS Recommendations

Bright Internet vs. CSIS Recommendations

3) Extend Deterrence and Create Consequences

7) Increased Transparency for Cyber Incidents

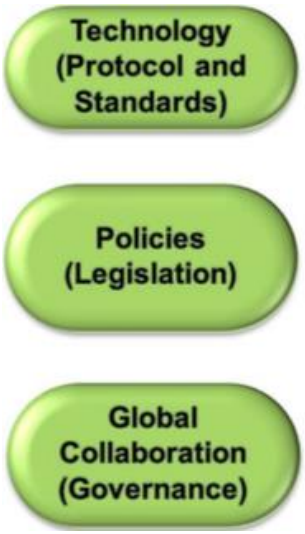
12) Increase the Cost to hackers

6) Enforce Privacy Policy for Data Protection and Privacy;

BI Five Principles

CSIS Recommendations

Bright Internet vs. CSIS Recommendations



8) Internet of Things

9) Encryption

11) Enhance baseline security by improving organizational governance for cybersecurity

13) Develop the close partnerships between U.S. military cyber forces and the intelligence community;

14) Use NETGuard, the National Guard, and the Reserves to protect critical assets in advance.

BI Solutions

CSIS Recommendations

Conclusions

- The similarities between the CSIS' recommendations and the Bright Internet recognize the need for global collaboration in cyber security.
- The complementary roles of each illustrate how academicians and policy makers can learn from each other and work together to create a safer global network.