

Making Democracy Harder to Hack



Prof. Scott J. Shackelford JD, PhD



KELLEY SCHOOL OF BUSINESS

INDIANA UNIVERSITY

Ostrom Workshop Program on Cybersecurity & Internet Governance

- **Goal:** *Applying polycentric principles to cybersecurity challenges*
- **Insight:** *Leverage nested governance structures that may be small in scope and scale, but start somewhere!*
- **Literatures:** *Regime complex, linkages, network effects, institutional analysis*
- **Potential Issues:**
 - *Fragmentation*
 - *Gridlock*
 - *Ethical and Political Pitfalls*

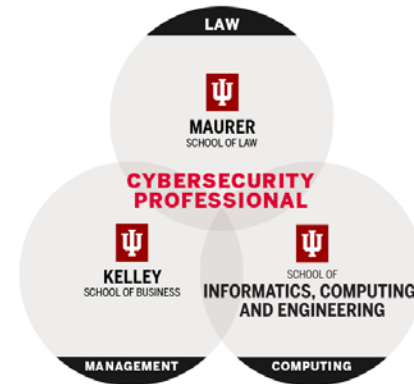


Ostrom Workshop



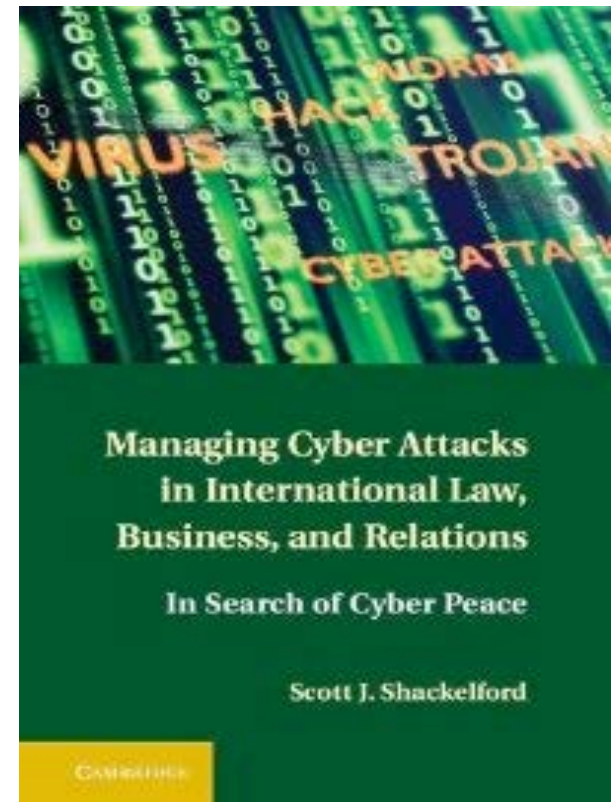
IU Cybersecurity Risk Management Program

- Multidisciplinary Program (Law, Secure Computing, & Business)
- Built on IU's Cybersecurity Certificates
- Applied Cybersecurity Risk Management Capstone
- Online courses available
- Cohort: 30+ (Fall 2017)
- Advisory Council



Objectives

1. **Breaking Down the Cyber Threat to Elections**
2. **Managing Cyber Attacks**
 - A. Identifying Threats
 - B. Regulatory Approaches
 - C. Cybersecurity Best Practices
3. **Securing Elections**
 - A. U.S. & E.U. Policy Options
 - B. Comparative Cyber Risk Mitigation Strategies
 - C. Role of International Law



Defining the Cyber Threat to Elections

To Companies

- Theft of IP is **Costly** – by some estimates (McAfee) more than \$400 billion annually
- **Widespread** – at least 19 million people in 120 nations
- **Easy** – more than 30,000 sites with malware available for download
- **Expanding** – Internet of (Every)thing

To Countries

- Fear of “Electronic Pearl Harbor” (overblown?)
- Protecting critical national infrastructure

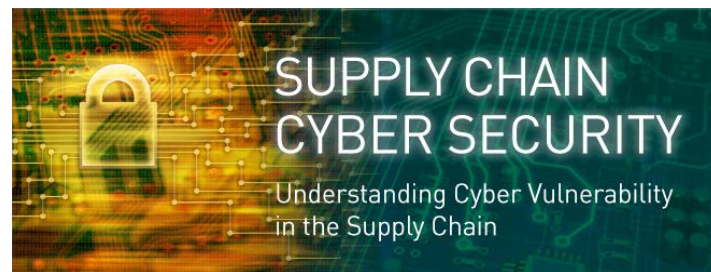


*Source: KAL's Cartoon, Economist, May 7, 2009

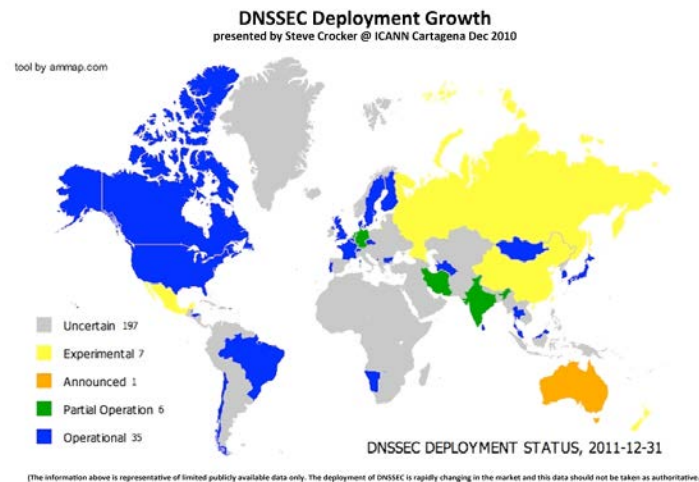
Managing Cyber Attacks

Technical Vulnerabilities

- Hardware
 - Secure Supply Chains
 - “Trust but Verify”
- Protocols
 - Ex: DNS
 - Importance of DNSSEC
- Code
 - Improving Accountability
 - Liability Issues
- Users



*Source: www.aronsonblogs.com



*Source: www.techbyte.pl

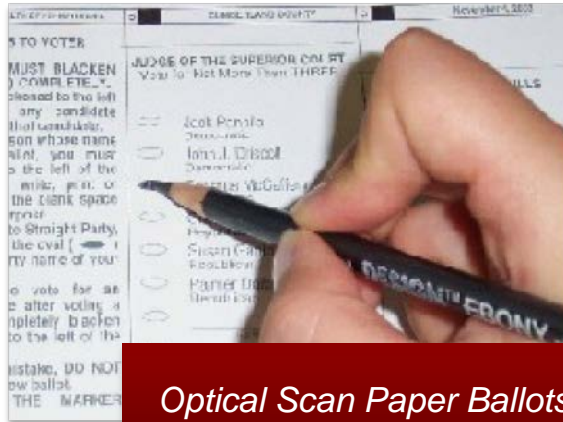
Private-Sector Cybersecurity Best Practices

- **Summary:** Be *proactive* and invest in built-in cybersecurity best practices from the inception of a project.
- **Technology**
 - Encrypt Data (at rest and in transit)
 - Biometrics & Deep Packet Inspection
- **Investments**
 - Average: >10-15% of IT budgets
 - Cybersecurity as CSR
- **Organization**
 - CISO Savings
 - Audit Training Programs & Penetration Testing

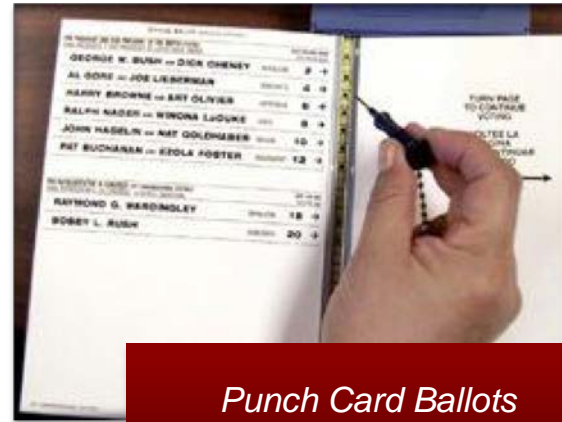


*Source: www.wizilegal.com

Application: Voting Technologies



Optical Scan Paper Ballots



Punch Card Ballots



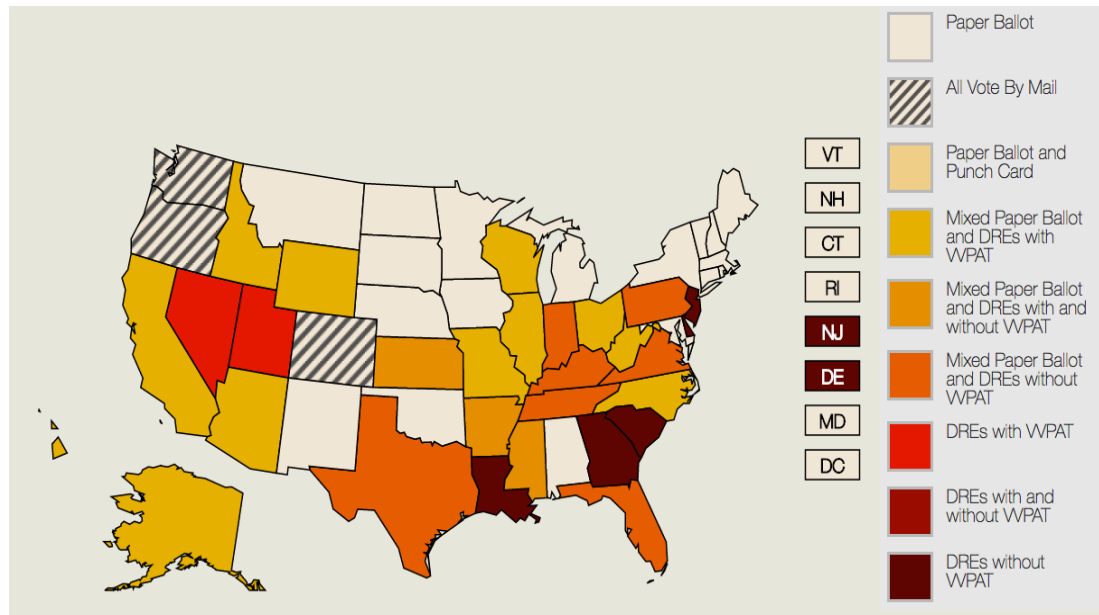
Direct Recording Electronic System (without Paper Audit)



Direct Electronic Voting Systems (with Paper Audit)

U.S. Voting Laws & Security Initiatives

- States largely control election processes and infrastructure



**Map from Verified Voting, www.verifiedvoting.org*

- 2002:** Help America Vote Act (HAVA) increased adoption of e-voting, but did not emphasize security
- 2016:** DHS offers voluntary assistance in response to infiltration of voter registration records
- 2017:** DHS designates election machinery as 'critical infrastructure'

Case Study: Hacking the 2016 U.S. Presidential Election

- **Vulnerabilities in the U.S. Election System**






- Voter Information
- Election Rolls
- Voting Machines
- Tabulation
- Dissemination
- Critical Infrastructure
- Internet of Things



- **Policy Responses**

- Keep Designation of Elections as ‘Critical Infrastructure’
- Federal Funding & Incentives
- NIST CSF Compliance, Deterrence, & Create a Voting ISAC

Voting Security – Comparative Approaches

County		Voting Processes	Security Challenges	Response
	South Africa	Paper ballots; Computer assisted tabulation	1994: Illicit computer program changed vote tally	Comprehensive reform and security updates
	Estonia	Internet voting with government ID card	2014: Experts identify major security risks	Dispute claims, but add security measures
	Germany	Paper ballots; EVM have been used in past	2009: Constitutional Court challenge to EV machines	Return to paper ballots
	Brazil	EVM; Discontinued use for financial reasons		
	India	EVM; Emphasis on security	2010: Experts identify vulnerability	Court ruling required voting verified paper trail

Recent EU Election Security Efforts

Recent Attacks

- 2016 Brexit Manipulation
- 2017 DoS Attacks against Netherlands, Bulgaria, and the Czech Republic
- 2017 Macron campaign breach
- 2018 cyber attacks on Bundestag

Responses

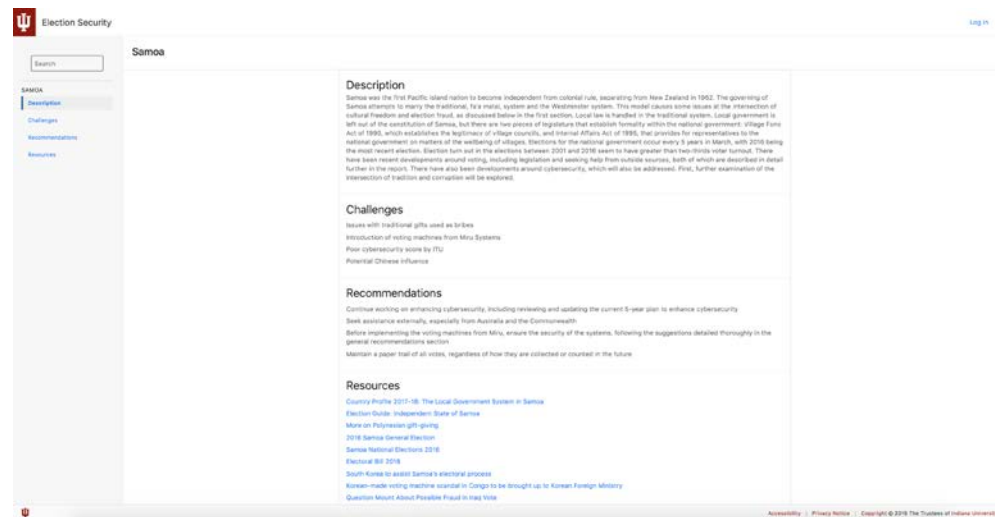
- Promoting use of paper ballots
- 2018 Compendium on Cyber Security of Election Technology
- 2018 Code of Practice on Disinformation
- Five Eyes Intelligence Sharing

Pacific Islands Comparison

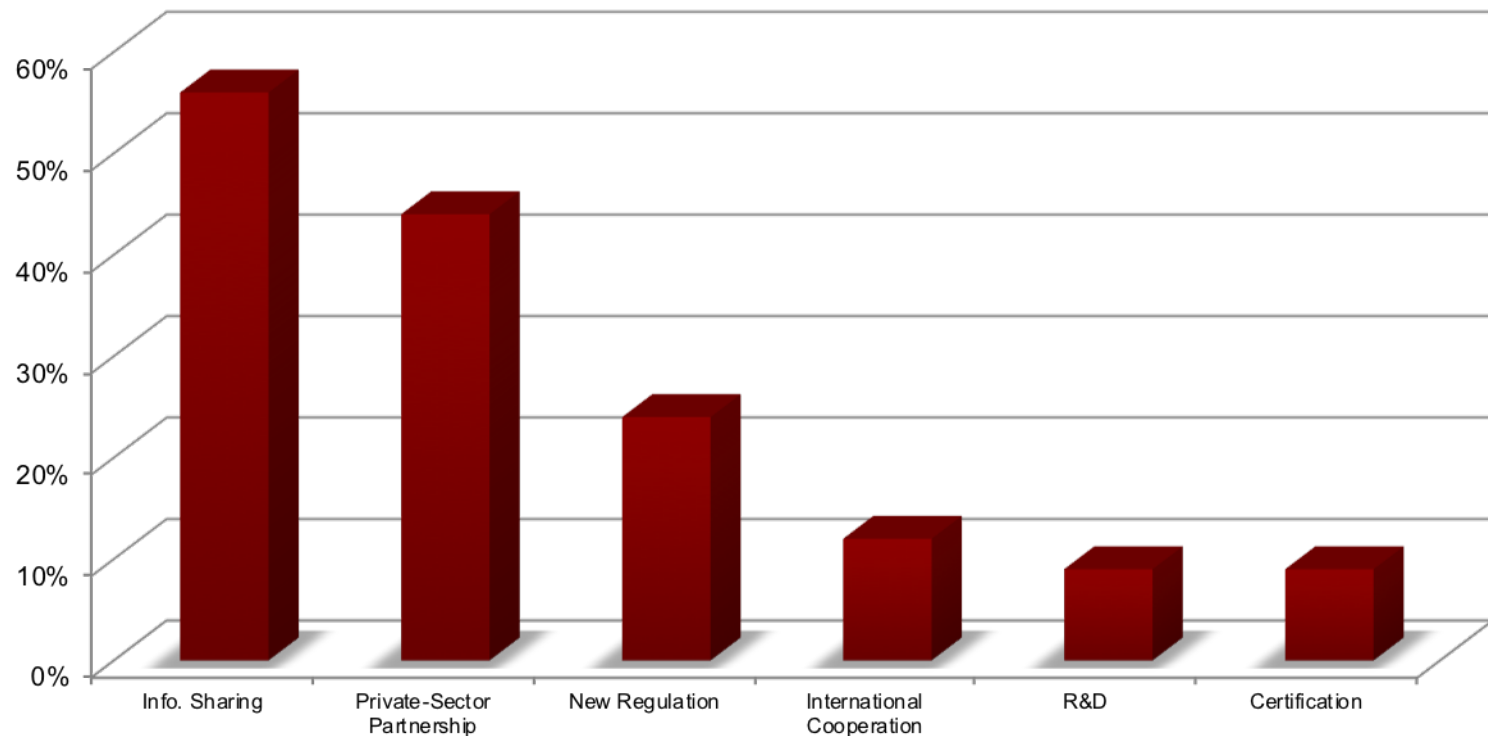
	Population	Voting Type	Electoral Roll	Absentee / Proxy Voting	Associations	Political Party Governance	Cybersecurity policy	Taiwan / China
Australia	23.4 Million	Paper	Electronic	Yes	Commonwealth	EAC	Yes	China
New Zealand	4.5 Million	Paper	Electronic	Yes	Commonwealth	Electoral Act	Yes	China
Micronesia	100,000	Paper	Paper		Compact of Free Association with US.	No	Yes	China
Fiji	900,000	Paper	Paper		Commonwealth			China
Kiribati	100,000	Paper	Paper	No	Commonwealth	No	No	Taiwan
Palau	20,000	Paper	Paper	Yes	Compact of Free Association with US.	No	No	Taiwan
Marshall Islands	75,000	Paper	Paper	Yes	Compact of Free Association with US.	No	No	Taiwan
Papua New Guinea	7 Million	Paper	Paper	Yes	Commonwealth	No	No	China
Samoa	200,000	Paper	Paper	Yes	Commonwealth	No	Yes	China
Solomon Islands	600,000	Paper	Electronic	No	Commonwealth	PPIA	No	Taiwan
Tonga	100,000	Paper	Paper	Yes	Commonwealth	No	No	China
Tuvalu	11,000	Paper	Paper		Commonwealth	No	No	Taiwan

Election Security Database

- **Goal:** Create an unbiased election security index to provide a resource to both emerging and advanced democracies.
- **Features:**
 - Expandable
 - Long-term project
 - Distributed



Critical Infrastructure Dimension Summary Chart



The NIST Cybersecurity Framework

- **2013 State of the Union Address**
 - Focus on cyber threats to nation's critical infrastructure
- **Executive Order 13636: Improving Critical Infrastructure Cybersecurity**
 - Increase information sharing
 - Ensure privacy and civil liberties protections
 - Develop a voluntary Cybersecurity Framework



*Source: welivesecurity.com

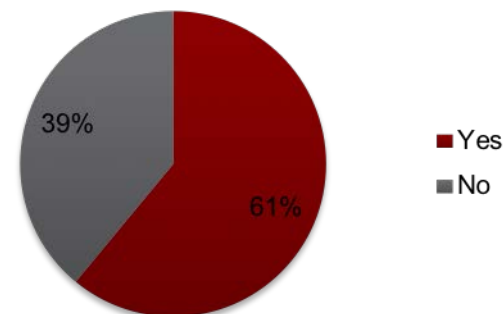
Regulating Cyberspace

- Governance Spectrum

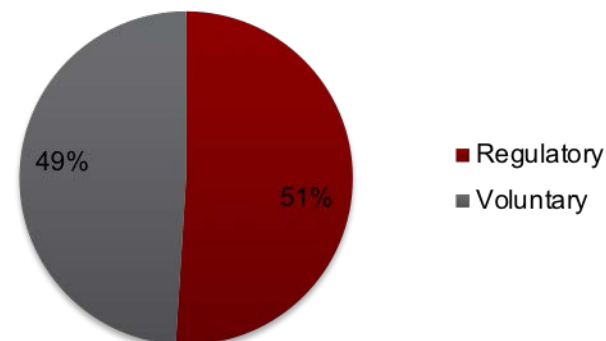


- Voluntary vs. Regulatory Approach

Suffered Cyber Attack in Past 12 Months?



Approach Favored in Managing Cyber Attacks?

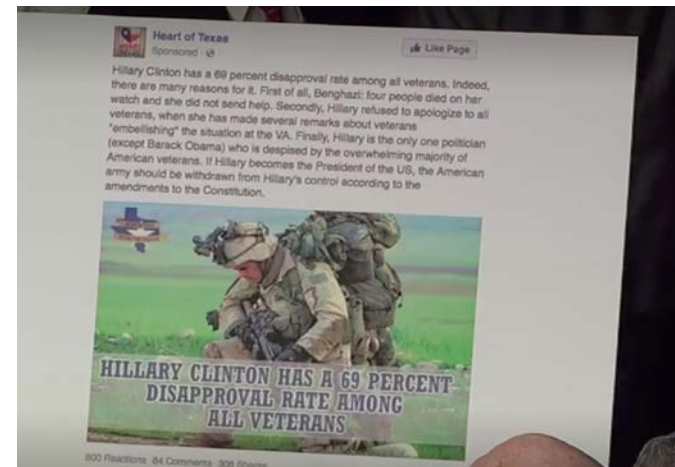


Combating 'Junk News' & Deep Fakes

Example #1



Example #2



Example #3: Eyes & Ears

Comparative Approaches to Combating Information Warfare

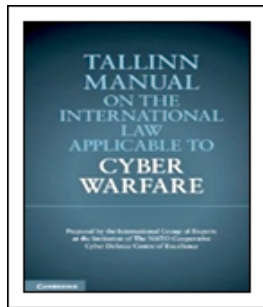
- ***Fighting “Fake News” in Italy***
- ***Addressing Disinformation D***
 - UK
 - Czech Republic
 - Ukraine
- ***Stopping “Fake News” by Making it news***
 - Do we need *more* “news” about “fake news”?
 - Lessons from Ukraine



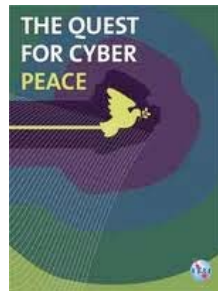
Role of International Law

- **Developments**

- Cybersecurity Norm Building
 - G2
 - G7
 - G20
 - UN GGE
- Intersection with Internet Governance



*Source: CCDCOE



*Source: ITU

- **Toward a Law of Cyber Peace?**

- **Countermeasures**
- **State Responses**
- **Analogies**
 - Nuclear War
 - Outer Space
 - Antarctica
- **Other Applicable Accords**
 - Mutual Legal Assistance Treaties
 - Vienna Convention on Diplomatic Relations
 - *Bilateral Investment Treaties*
- **Summary:** *It's a patchwork, but it's a beginning!*

Defining “Cyber Peace”

Vatican’s Pontifical Academy of Sciences Erice Declaration on Principles for Cyber Stability and Cyber Peace

1. All governments should recognize that **international law guarantees individuals the free flow of information and ideas**; these guarantees also apply to cyberspace. Restrictions should only be as necessary and accompanied by a process for legal review.
2. All countries should work together to **develop a common code of cyber conduct and harmonized global legal framework**, including procedural provisions regarding investigative assistance and cooperation that respects privacy and human rights. All governments, service providers, and users should support international law enforcement efforts against cyber criminals.
3. All users, service providers, and governments should work to ensure that **cyberspace is not used in any way that would result in the exploitation of users**, particularly the young and defenseless, through violence or degradation.
4. Governments, organizations, and the private sector, including individuals, should implement and maintain **comprehensive security programs based upon internationally accepted best practices** and standards and utilizing privacy and security technologies.
5. Software and hardware developers should strive to develop **secure technologies that promote resiliency** and resist vulnerabilities.
6. Governments should actively participate in **United Nations’ efforts to promote global cyber security and cyber peace** and to avoid the use of cyberspace for conflict.

Paris Call for Trust and Security in Cyberspace

- 7 principles, including election security)
- 564 official supporters, including 67 nations
- Benefits/Draw backs?

Indiana University among first to endorse Paris Call for Trust and Security in Cyberspace

FOR IMMEDIATE RELEASE

Nov. 12, 2018



BLOOMINGTON, Ind. -- Indiana University has joined in endorsing the [Paris Call for Trust and Security in Cyberspace](#), a document calling for international cooperation in the realm of cybersecurity, presented today by French President Emmanuel Macron at the Paris Peace Forum.

The declaration was made at the [13th annual meeting of the Internet Governance Forum](#), hosted by the French government at the headquarters of UNESCO in Paris. Because of its leadership in the area of internet governance and cybersecurity, IU was encouraged to be an early signatory of the document along with universities in Asia and Europe and research centers affiliated with universities around the world.

"As a world leader in the uses and applications of information technology and in computer networking, Indiana University is pleased to join in supporting this tremendously important initiative," IU President Michael A. McRobbie said. "As noted in the opening comments of today's declaration, cybersecurity is crucial in all aspects of



Referenced Papers

1. ***Defending Democracy*** (working paper)
2. ***Making Democracy Harder to Hack: Should Elections be Classified as ‘Critical Infrastructure?’***, 50 MICHIGAN JOURNAL OF LAW REFORM 629 (2017) (with Michael Sulmeyer, Bruce Schneier, Anne Boustead, Ben Buchanan, Amanda Craig, Trey Herr, & Jessica Malekos Smith)
3. ***A State-Centric Cyber Peace? Analyzing the Current State and Impact of National Cybersecurity Strategies on Enhancing Global Cybersecurity***, 18 NEW YORK UNIVERSITY JOURNAL OF LEGISLATION AND PUBLIC POLICY 895 (2016) (with Andraz Kastelic)
4. ***Bottoms Up: A Comparison of “Voluntary” Cybersecurity Frameworks***, 16 UNIVERSITY OF CALIFORNIA DAVIS BUSINESS LAW JOURNAL 217 (2016) (with Scott Russell & Jeffrey Haut)
5. ***Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices***, 50 TEXAS INTERNATIONAL LAW JOURNAL 287 (2015) (with Andrew Proia, Amanda Craig, & Brenton Martell).

Discussion Questions

1. Should political party infrastructure be classified as critical infrastructure along with voting machines?
2. Is a new forum needed to catalyze the development of new international cybersecurity norms, including those relating to critical infrastructure? If so, what form should that take?
3. Do voting machine manufacturers and other vendors have a social responsibility to boost security absent regulatory interventions?
4. How can we build resilience among citizens to help ward off information warfare campaigns?
5. What does “cyber peace” mean to you?

Questions?

Contact Info

sjshacke@indiana.edu