What Do Social Scientists Know About the Laws and Policies Related to Cyber Trespass?

Created by: Amiah Armstrong, Jasmyn Wilhelm, and Louis Ferrara

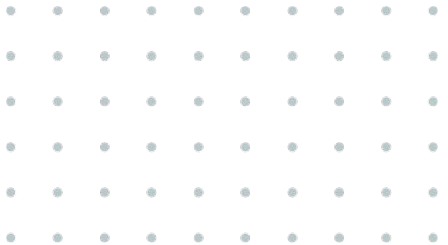
TABLE OF CONTENTS

INTRODUCTION

Cyber trespass raises significant legal and ethical concerns in a digital society. As technology evolves, regulations to protect individuals and organizations from unwanted access to digital environments change. Social scientists offer valuable insights into the definition, laws, and enforcement of cyber trespass.

The present status of cyber trespass laws and practices is examined in this presentation, with particular attention paid to the socioeconomic effects, legislative obstacles, and public opinion. This research intends to comprehend how social science, by combining knowledge from other specialist areas, improves our understanding of cyber trespass and its social implications, thereby enhancing our understanding of cyber law.

You can examine the complex relationships between law, technology, and social behavior by using our insights on the state of the art and new directions in modern governance.

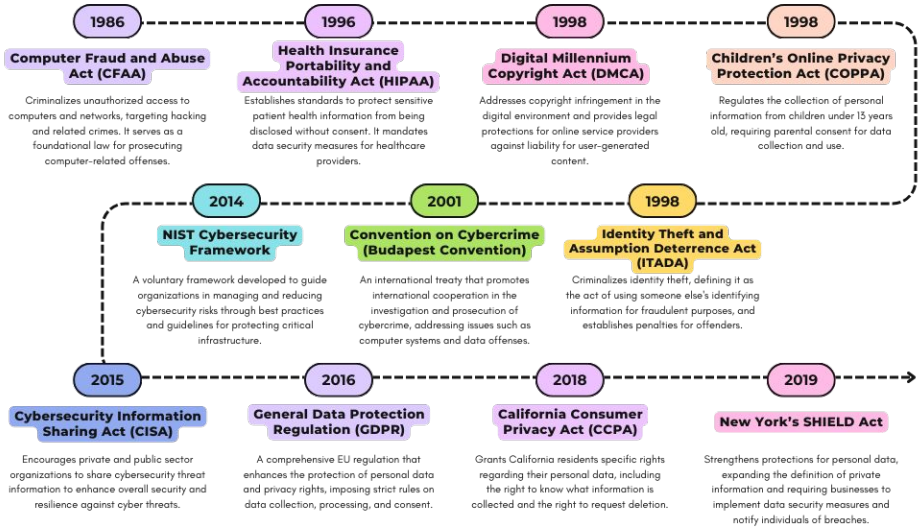


Cybertrespass in Relation to Cybercrime and Digital Deviance

How Are Laws Evolving For Cyber Threats?

Cybertrespass laws, like the Computer Fraud and Abuse Act (CFAA), focus on purpose and potential harm in order to stop hostile behaviors like hacking and virus spread. They fall under the category of cybercrime and include illicit acts such as phishing and identity theft. Since cybercriminals frequently take advantage of anonymity and jurisdictional borders, enforcement issues complicate this link. In order to standardize regulations, effective policies place an emphasis on prevention through international cooperation and education. Significant cyber events emphasize how crucial it is to modify legislation to respond to the changing digital environment.

Timeline



01.

Article I

Analyzed by: Jasmyn Wilhelm

“Why has the U.S. not taken a similarly strong approach to privacy management and regulation?” (Holt, n.d.)

Data Privacy Rules In the EU May Leave the US Behind

Inspired by Thomas Holt

For violating the General Data Protection Regulations (GDPR), Google was slammed with a $57 million fine by France. This is the first time that a penalty of this size has been applied. Due to its lack of transparency on the collection and use of user data, Google was penalized. Similar investigations into Facebook, Instagram, and WhatsApp are still occurring in the EU. The US remains behind Europe with putting similar privacy management and rules into place. Despite the fact that most of the biggest internet service providers in the world are based in the US, it seems as though the EU has taken on increased oversight authority. In the US, there has been an immediate threat to the privacy of individuals' personal information and the power of government agencies tasked with investigating cybercrime.

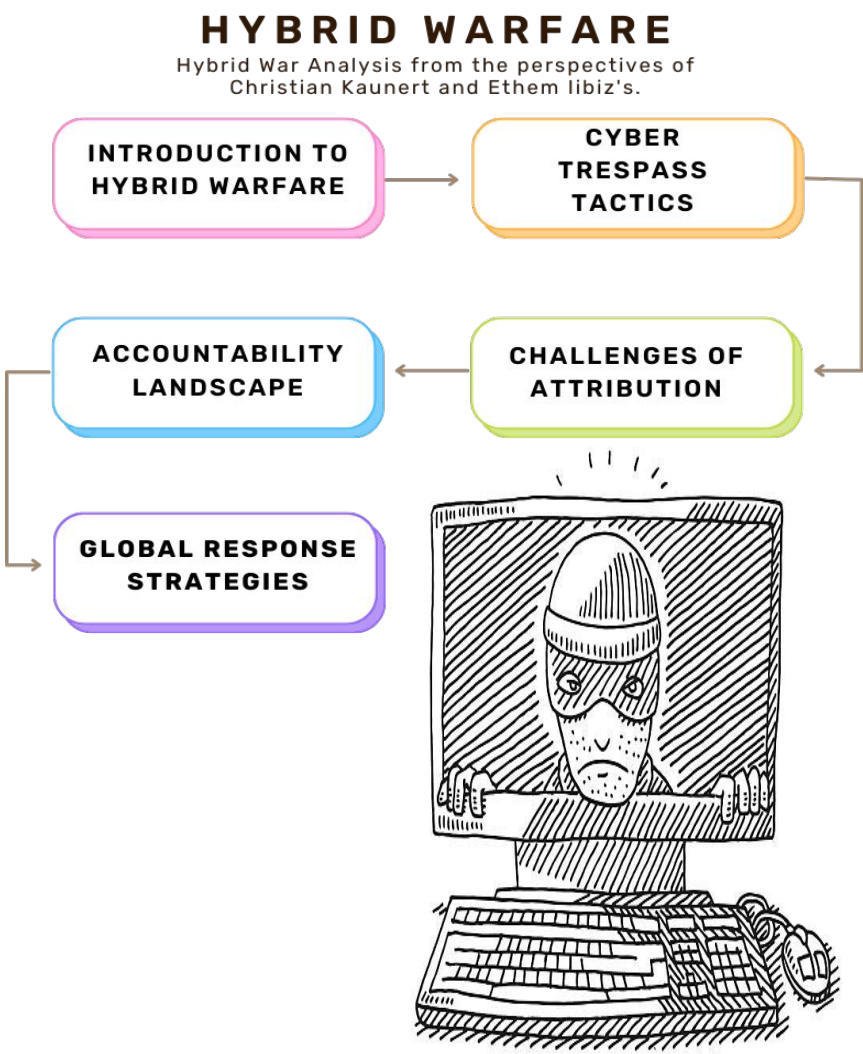
02.

Article II

Analyzed by: Louis Ferrara

Cyber-Attacks: What Is Hybrid Warfare and Why Is It Such A Threat?

To achieve political objectives, hybrid warfare combines traditional military measures with non-conventional methods like disinformation campaigns and cyberattacks. The goal of cyber trespass methods like ransomware and hacking is to weaken public confidence and disturb critical systems. Responses are made more difficult by the attribution problem since attackers frequently act in secret, making it hard to pin down the perpetrators. There are at times challenges in duty because private businesses face the greatest burden of accountability. As a result, the US and the EU are creating extensive plans to strengthen cyber resilience and combat the growing threat of hybrid warfare. These plans include joint defense projects and penalties.



03.

Article III

Analyzed by: Amiah Armstrong

Why Cyber Defense is a "Wicked" Problem

Terry Thompson's view on the current state of our U.S. National Cyber Defense

THE CATALYST

COLONIAL PIPELINE

- This Infrastructure controls most of the East Coast's liquid fuels.
- Ransomware attack on infrastructure.

SOLARWINDS

- One of the most devastating cyber attacks in history.
- Revealed weaknesses in international software supply networks.

BOTH WERE COMPROMISED BY VERY COMMON CYBER ATTACKS!

THE "WICKED" PROBLEM

Thompson suggests our cyber defense is not taking cybersecurity as serious they should.This is evident from the mention SolarWind's failure to practice basic cybersecurity hygiene, and the lack of software engineers in America. He highlights the fragmented authority over cybersecurity responsibilities. This in general, leaves gaps in our national defense and complicates protecting our critical systems.

He believes there are too many weaknesses in the U.S. defenses, many of them coming from the lack of effort to protect online systems.

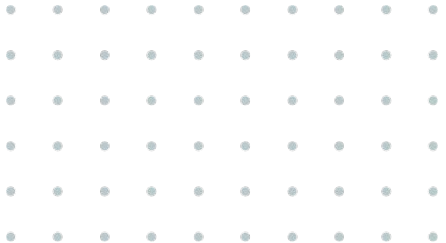
REVITALIZED POLICIES

The establishment of a national cybersecurity director was a good step, but not enough. Thompson believes we need…

1. Better policies to enhance coordination among various agencies
2. Continued assessment of vulnerabilities and proactive security measures.
3. Robust policies that require regular security audits, red-teaming exercises, and collaboration between public and private sectors and organizations.
4. Creating a comprehensive policy framework would not only improve overall cybersecurity resilience but also foster a culture of accountability and vigilance against evolving threats.

CONCLUSION

In an increasingly digital world, the legal and ethical issues surrounding cyber trespass continue to evolve, and regulators refuse to catch up. Cybercriminals take advantage of the outdated systems of our important infrastructures. The United States is being hit with fines for their lack of accountability and privacy management. The cyber attacks a normal civilian encounters regularly are now also warfare tactics. Times are changing rapidly, and the gap between evolving threats and regulatory response is widening. Thomas Holt, Terry Thompson, Ethem Iibiz, and Christian Kaunert may all be experts in their specified field, but there is one thing these researchers can all agree on: The United States is too far behind on policy, regulation, and defensive strategies. More concerted efforts are needed to keep our infrastructures and citizens safe.



REFERENCES

Graham, R.S., & Smith, '.K. (2024). Cybercrime and Digital Deviance (2nd ed.). Routledge. https://doi-org.proxy.lib.odu.edu/10.4324/9781003283256

Holt, T. (n.d.). *Data privacy rules in the EU may leave the US behind*. The Conversation. https://theconversation.com/data-privacy-rules-in-the-eu-may-leave-the-us-behind-110330

Kaunert, C., & Ilbiz, E. (2021, July 21). *Cyber-attacks: what is hybrid warfare and why is it such a threat?* The Conversation. https://theconversation.com/cyber-attacks-what-is-hybrid-warfare-and-why-is-it-such-a-threat-164091

REFERENCES Continued…

McNicholas, E. R., & Angle, K. J. (2023, November 14). *Cybersecurity Laws and Regulations USA 2024*. International Comparative Legal Guides International Business Reports. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa

Product details 97-1025. (n.d.). https://crsreports.congress.gov/product/details?prodcode=97-1025

Thompson, T. (n.d.). *The Colonial Pipeline ransomware attack and the SolarWinds hack were all but inevitable – why national cyber defense is a 'wicked' problem*. The Conversation. https://theconversation.com/the-colonial-pipeline-ransomware-attack-and-the-solarwinds-hack-were-all-but-inevitable-why-national-cyber-defense-is-a-wicked-problem-160661

The end.

Department of Sociology and Criminal Justice, Old Dominion University
CRJS/CYSE 310: Cybercrime: Foundations
Dr. Roderick Graham