The Evolving Demands of a Data-Driven Society: 
The New Cyber Challenge

J.S. Hurley, PhD
The 14th International Conference on Cyber Warfare and Security 
(ICCWS) 2019
Stellenbosch South Africa

National Defense University
Washington, DC, USA
Abstract

The stages of evolution that we see in our society continue to be connected to parallel advancements in technology. As sources capable of generating data expand beyond traditional IP devices, e.g., the Internet of Things (IoTs), data will be more pervasive in driving many of the key decisions in our lives. Our increasing reliance on data will be of particular interest as it will provide unquestionable benefits, but unfortunately also some very difficult challenges. In this presentation, we will examine some of the new developments and challenges of a data-driven society and the need to look differently at cybersecurity, national security and the preparation of the future workforce.
Data Proliferation and Some Challenges

- Everyday, we create 2.5 quintillion bytes of data.
- 90% of the data in the world today has been created in the last two years.
- Unstructured data could form as much as 80-90% of an organization's overall data.
- 85% of IT Professionals store their data in different locations.
- 68% of IT Professionals said their IT complexity was increasing.
- 35% of IT professionals use 6+ products to manage their secondary data.
U.S. Government Data Explosion

- The data explosion challenges caused by the sheer influx of data require data driven solutions
- Data has a lifespan that can render it inaccurate or irrelevant
- Federal government seeks to establish data hygiene and categorization practices to handle the data explosion

Source: www.scality.com
Social Media: Every Minute of the Day

• 49,380 videos are uploaded to Instagram
• 2,083,333 snaps are sent on Snapchat
• Nearly 25,000 GIFS are sent on Facebook Messenger
• 473, 400 tweets are sent on Twitter
• 12,986,111 texts are sent
• Spotify streams over 750,000 songs

www.psychologytoday.com; https://www.domo.com
Drivers

• ‘Data is shaping all aspects of our society’, including how key decisions are made

• Big data allows us to connect the ‘dots’ that provide good indications of future behavior – key requirement for success for senior decision makers (especially with regards to cyber events)

• To gain the necessary insight, we need to employ models that incorporate fine-grained details of societal interactions
Data-driven Society

• Key
  o Data must be treated as an asset in which individuals have ownership rights in data about them

• Rights:
  o Possess data about self
  o Full control over use of own data
  o Dispose of or distribute own data
Background

• **Data**
  - Collection of descriptions, observations and facts
  - Raw, unorganized, unprocessed, unstructured

• **Information**
  - Data transformed in a way to meet specific needs
  - Refined, organized, processed, structured

• **Data-driven**
  - Decision-making approach that views data as critical evidence that informs and influences strategy

• **Success**
  - Senior leaders can recognize data trends and patterns that enable them to make informed choices
How Can Cyber Attacks Hurt National Security?

- Government policies for information sharing remain vague
- New tools, such as social media platforms, are being used to manipulate information

https://www.reuters.com
Cyber-attacks are Risks for National Security

- Data growth and democratization represent two game-changing trends on cybersecurity
- Much larger attack surface created and must be defended (External)
- More than 40% of all data breaches perpetrated from inside (Internal)

https://thenewsversion.com
Understanding Cyber Threats and Vulnerabilities

• Must maximize the inherent value of data while ensuring its safety

• The existence of a risk requires a threat/vulnerability pair,
  • In other words, there has to be both a threat and a vulnerability for a risk to exist

• Malware continues to loom as a primary feature of the threat landscape
  • However, it is often only the precursor to an attack, not the ultimate objective

https://www.mdcyber.com
Smarter Enemies Alter Cyber Battlefield

- New TTPs are adopted by adversaries
  - Long-running strategic web compromise (SWC) campaigns,
  - Mobile malware, and
  - Publicly disclosed information operations on Western social media platforms
- Health-related misconceptions, misinformation, and disinformation spread over social media, posing a threat to public health
- There is an increase in the shift in cyber threat focus from PII and credit cards to the destruction of networks

https://www.govtechworks.com
World’s Biggest Data Breaches in History and Motivation

https://www.easyuni.com
Cycle of Challenges
Building the Next Generation of Cyber Warriors

- Currently, cyber breaches are costing the U.S. more than $100 billion a year
- Global shortage of almost 2 M cybersecurity professionals this year
- Introduce Cybersecurity into All Disciplines
- Leverage the Right Certifications
- Align Curriculum with National Cybersecurity Guidelines

https://www.cio.com; https://www.securitymagazine.com
Cyber Attack

• A cyber attack is any type of offensive action that targets:
  • computer information systems,
  • infrastructures,
  • computer networks, or
  • personal computer devices using various methods to steal, alter or destroy data or information systems. (https://blog.netwrix.com)

• A cyber attack is a strike against a:
  • computer system,
  • network, or internet-enabled application or device.

https://www.inc.com
Existing Approach

- Team of scholars (MIT) views companies and governments as ‘ideas machines’
- Machines harvest and spread ideas through individual interactions
- Focus on two mathematical patterns for healthy idea flow
  - Engagement
    - Person-to-person interactions within a group that regularly occurs
  - Exploration
    - Mathematical measure of how group members bring in ideas from the outside
- Track employees via electronic devices
Proposed Approach

• Hierarchical pairwise comparison of criteria and alternatives to rank cyber threat actors
• Approach takes down to individual level
• Key surprise of some of the candidates and how they are ranked
Sensitivity Analysis
Tradeoff Analysis
Recommendations

• Focus on ‘Smart Big Data’ instead of ‘Big Data’
  • Define the questions that need answering then collect and analyze only that data which answers the question

• Human Factor
  • In the most successful AI deployments, humans are regularly used to cooperate with machine learning and deep learning algorithms to improve accuracy
  • Some times humans get it right and machines don’t

• Treat the private sector as a ‘crime scene’ where often cyber threats begin
  • A lot about malicious actors can be learned from partnerships between the private sector and the government
Conclusions

• Understanding the interactions of society can help us predict future behavior patterns and in particular threats to information sharing

• The sole focus on cyber (only in the context of systems) has pulled us away from a very critical information threat

• Introduce Cybersecurity into All Disciplines

• Social media platforms will continue to be one of the largest data generating sources of our future and society must understand the dual nature

• A hierarchical model can provide insight that ranks cyber threats to an organization
Q&A and Acknowledgements

• Thank You

• Q&A

• Very special thanks to Noelle, Louise, Sue, CSIR, the National Research Foundation and relevant administration, peers and staff for their invaluable support and consideration. Special thanks to Ms. Bahedile Lefoka and Ms. Yvette Zietsman for their patience and consideration.

• Please note that the opinions expressed in this presentation do not reflect a view of the US Government, Department of Defense, or the National Defense University. They are only those of the presenter.