The Past, Present, and Future of the Cyber Domain

Dr. Andrew W. Reddie
areddie@berkeley.edu; @areddie89
University of California, Berkeley
Goldman School of Public Policy

Berkeley Public Policy
The Goldman School

UC Berkeley
Risk & Security Lab

Berkeley
UNIVERSITY OF CALIFORNIA

Brief Introduction

I am a scholar of international relations working at the intersection of technology, politics, and international security issues.

Research: Nuclear weapons, AI governance, cybersecurity, civ-mil relations, political methodology and wargaming

Teaching: War? Emerging Tech and National Security Policy; Nuclear Security; Intro to Technology and Public Policy; Quantitative Methods

Affiliations (selected):

- Founder, Berkeley Risk and Security Lab
- Director, Center for Security in Politics
- Senior Director, Bridging the Gap

Setting the Stage

- Digital transformation across every sector (gov, defense, finance, healthcare)
- Growing attack surface (cloud, mobile, IoT, operational tech, AI)
- Nation-state competition + criminal ecosystems
- **Cyber as a domain of strategic competition (Russia, China, Iran, DPRK)**

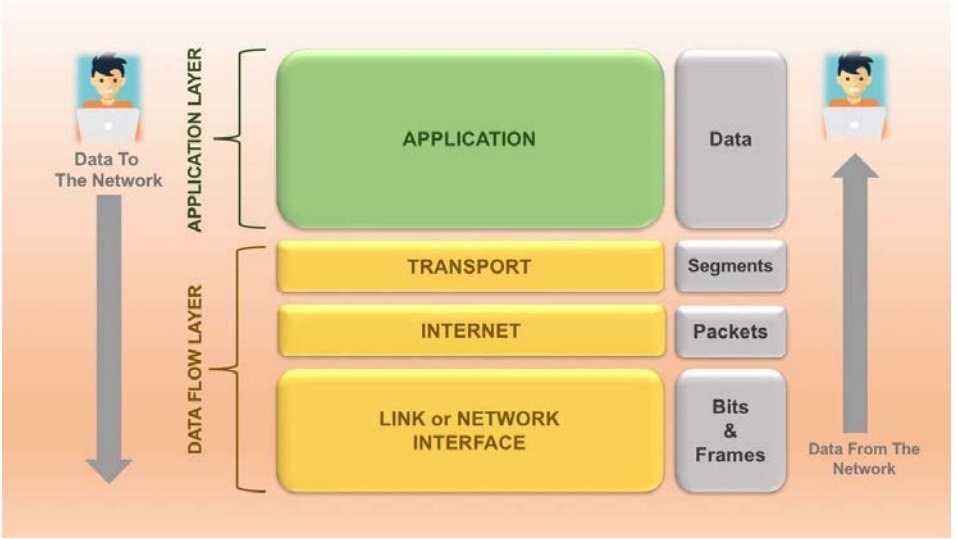
The Source of Vulnerability

How should we think about the Internet?

There are vulnerabilities across each of these layers;

Risk = Threat * Vuln * Consequence

- Probabilities and policy…



From Script Kiddies to State Actors

- Cybercrime and ransomware
- Supply-chain compromises
- Critical infrastructure vulnerabilities
- Hybrid warfare (cyber + info ops + kinetic)
- Nation-state operations

The Spectrum of State Responsibility

There are a variety of different ways for states to ostensibly engage in cyber attacks:

- State-prohibited
- State-prohibited-but-inadequate
- State-ignored
- State-encouraged
- State-shaped
- State-coordinated
- State-ordered
- State-rogue-conducted
- State-executed
- State-integrated

Core Concepts: The “Other CIA”

At the application layer, the CIA triad—*Confidentiality*, *Integrity*, and *Availability*—represents the core principles of information security. **Confidentiality** ensures that sensitive information is accessible only to authorized users, protecting it from unauthorized access or disclosure.

Integrity maintains the accuracy and trustworthiness of data by preventing unauthorized alterations, while **Availability** guarantees that information and systems are accessible when needed, ensuring the continuous functioning of services.

The Cyber Domain and State Competition

Across all layers, the cyber domain in modern warfare has become a critical battleground where states and non-state actors engage in offensive and defensive operations to **disrupt**, **degrade**, or **control** information systems and critical infrastructure.

Cyber operations can range from **espionage** and **sabotage** to influence campaigns and full-scale attacks on military and civilian targets, often blurring the lines between peace and conflict.

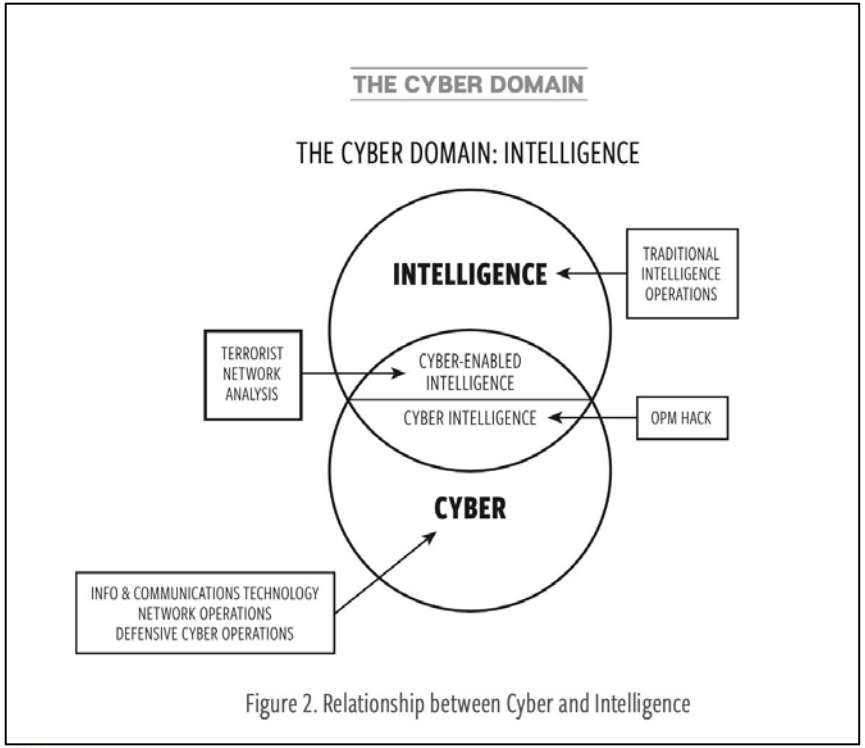
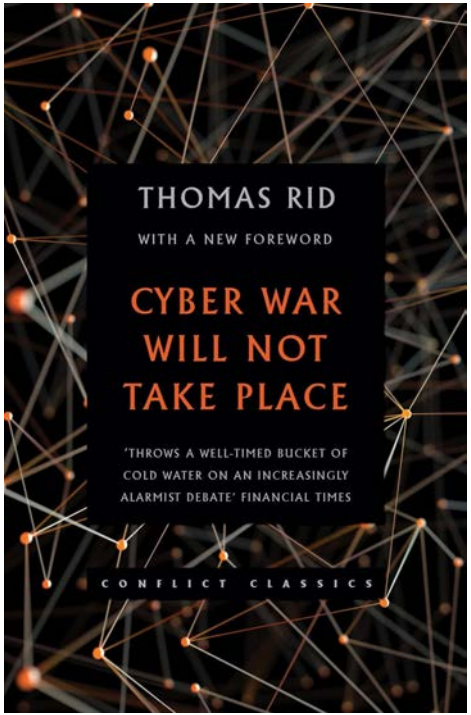


Figure 2. Relationship between Cyber and Intelligence

On Cyber War: Has cyber war taken place?

As is often the case, there is scholarly debate surrounding the degree to which cyber war has, is, or will take place…

… and where **intelligence** ends and **war** begins.



What's New: The Attribution Problem

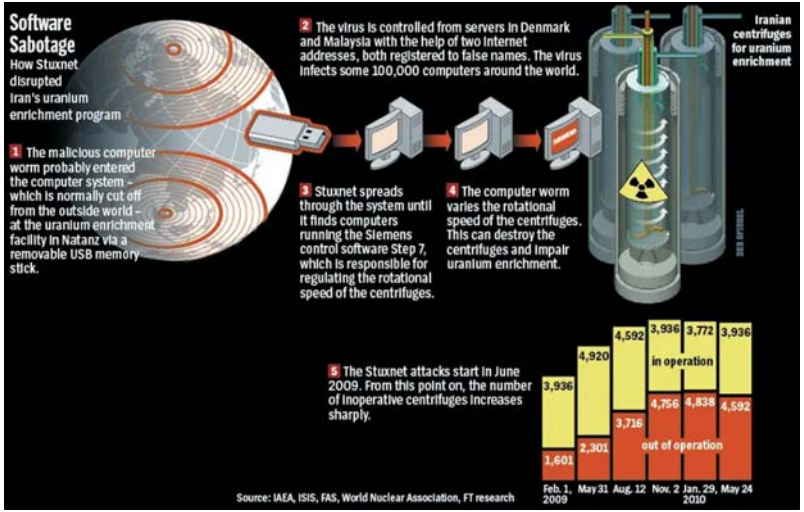
Unlike conventional warfare, where the origin of an attack is often easily traced to a specific nation, group, or individual, cyberattacks can be difficult to attribute:

- Attackers can use various methods to hide their identities, such as proxy servers, encryption, and the use of compromised third-party systems (botnets)
- Attackers can deliberately leave misleading evidence (such as using specific code signatures or languages) to frame other actors or deflect attention from their true identity (**false flags**)
- A relatively **high threshold for proof** as well as **political** concerns

Examples: Stuxnet (and Kinetic Effects)

The Stuxnet cyber attack, discovered in 2010, was a sophisticated computer worm believed to be jointly developed by the U.S. and Israel to sabotage Iran's nuclear enrichment program. It specifically **targeted programmable logic controllers** (Siemens PLCs) used in Iran's Natanz facility, causing physical damage to centrifuges by **altering their operational speeds** while reporting normal functioning to operators.

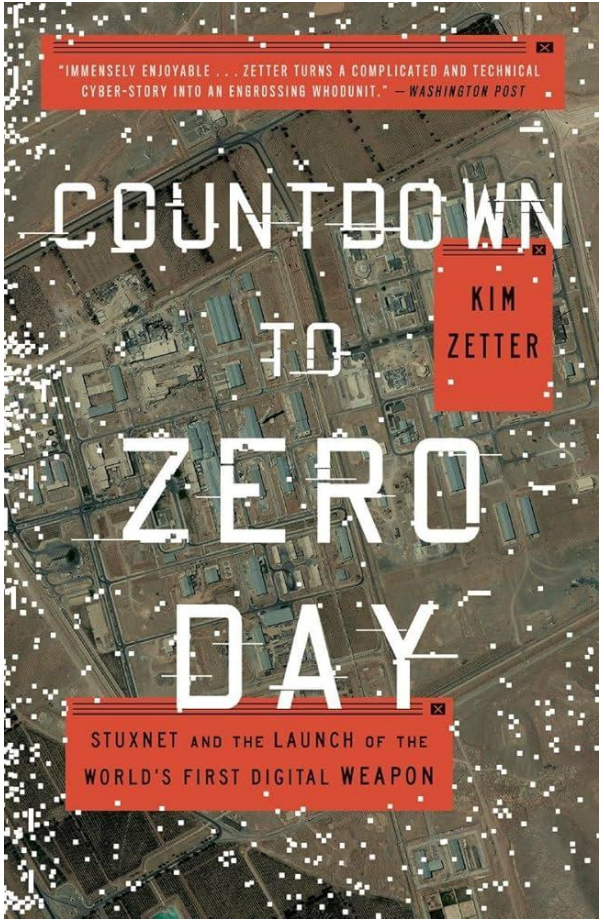
Stuxnet marked a turning point in cyber warfare, being one of the first known instances of a cyber weapon causing **physical damage** to critical infrastructure.



Examples: Stuxnet

The Stuxnet cyber attack, discovered in 2010, was a sophisticated computer worm believed to be jointly developed by the U.S. and Israel to sabotage Iran's nuclear enrichment program. It specifically **targeted programmable logic controllers** (Siemens PLCs) used in Iran's Natanz facility, causing physical damage to centrifuges by **altering their operational speeds** while reporting normal functioning to operators.

Stuxnet marked a turning point in cyber warfare, being one of the first known instances of a cyber weapon causing **physical damage** to critical infrastructure.

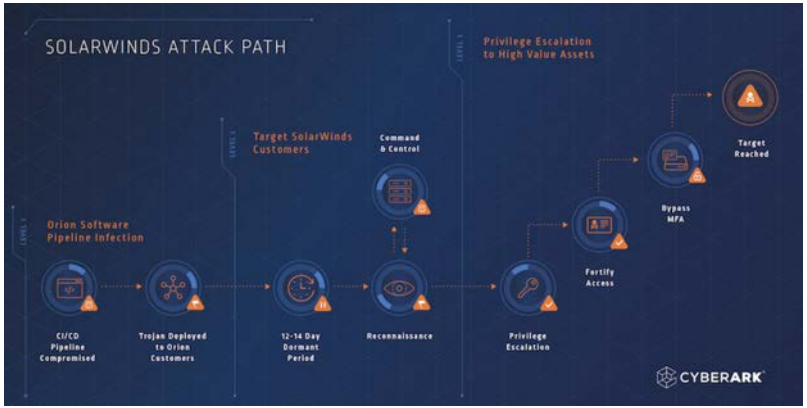


Examples: SolarWinds

Russian intelligence (APT29/Cozy Bear) compromised SolarWinds Orion software updates.

Malicious update distributed to ~18,000 customers, including U.S. government and Fortune 500 firms.

- Demonstrated stealth, patience, and sophistication of state APTs.
- Hard problem: defenders must secure entire chain; attackers can exploit a single weak link.
- "**Defend forward**" and zero-trust architectures become core conversation. [Can companies "hack back"?]
- Requires deep visibility into CI/CD pipelines.
- Supply-chain attacks avoid traditional perimeter defenses.
    - Illustrated the fragility of trust in global software supply chains.



Examples: Oldsmar

The Oldsmar attack in February 2021 was a cyber intrusion into a **water treatment facility** in Oldsmar, Florida, where hackers remotely attempted to increase the levels of sodium hydroxide (lye) to dangerous amounts. The attack was detected and reversed by a plant operator, preventing harm to the public.

This incident underscored the risks to public safety posed by cyberattacks on critical infrastructure, particularly in small or poorly resourced facilities.

**Note the IT/OT gap...

Examples: Bowman Avenue Dam

- The 2013 Bowman Avenue Dam intrusion—often referred to as the Rye Brook dam attack—was an early and highly publicized example of Iranian cyber operations targeting U.S. critical infrastructure.
- Hackers linked to Iran's Revolutionary Guard Corps gained unauthorized access to the small flood-control dam's SCADA system **exploiting a vulnerability in a remote access interface**.
- The incident served as a strategic wake-up call, revealing that even minor facilities can be entry points or testbeds for future attacks and highlighting the growing willingness of states to use cyber tools to surveil and potentially disrupt civilian infrastructure.
- IRGC likely confused with Arthur R. Bowman Dam on the Crooked River in Oregon

Examples: Colonial Pipeline

The Colonial Pipeline attack in May 2021 was a ransomware attack carried out by the criminal group DarkSide, which targeted the IT systems of the largest fuel pipeline in the United States. The attack forced the company to shut down its operations for several days, causing widespread fuel shortages across the East Coast.

The incident highlighted the vulnerability of critical infrastructure to cyberattacks and led to increased government focus on cybersecurity in the energy sector.

Volt Typhoon: Pre-positioning in U.S. Critical Infrastructure

PRC-linked threat actor infiltrated U.S. critical infrastructure networks (power, water, communications).

- Focus on stealthy access, living-off-the-land techniques (no malware).
- Aimed at enabling disruptive capabilities in crisis or conflict.
- Represents shift from espionage to **preparation of the battlespace**.
- This is *strategic*: shaping potential conflict outcomes by holding civilian infrastructure at risk.

Key lessons:

- Detection is challenging without malware indicators.
- Incident demonstrates the importance of logs, segmentation, and OT security.
- Raises questions about deterrence, signaling, and crisis stability.

Cyber and the War in Ukraine

Source: Microsoft Digital Security Unit

Cyber and the War in Ukraine

Note the coupling of cyber and military operations…

Epilogue: The Introduction of “AI”

Lowering the barriers to entry for threat actors of all types;

Automating both cyber defense and cyber offense (a new “arms race”);

And the LLMs, themselves, have vulnerabilities (“**data poisoning**”)

- Open data; open weights

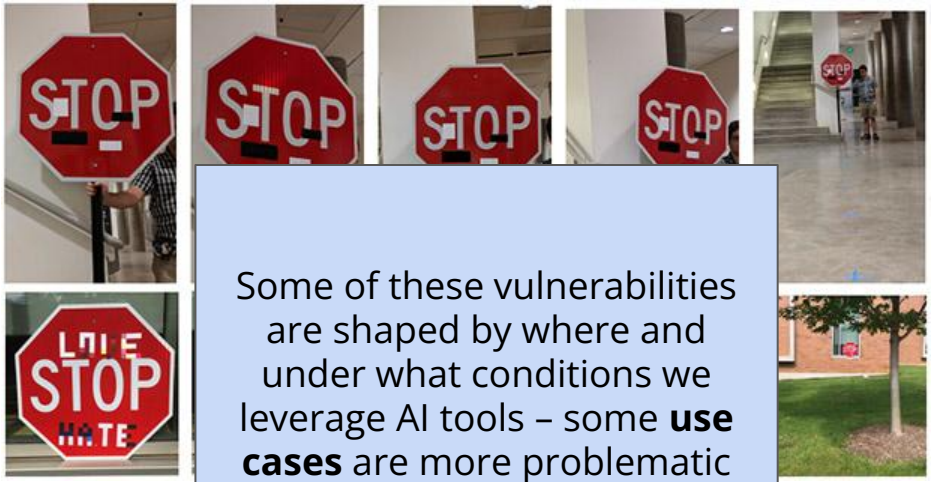
The Introduction of “the AI”

Lowering the barriers to entry for threat actors of all types;

Automating both cyber defense and cyber offense (a new “arms race”);

And the LLMs, themselves, have vulnerabilities (“**data poisoning**”)

- Open data; open weights



Some of these vulnerabilities are shaped by where and under what conditions we leverage AI tools – some **use cases** are more problematic than others…

The Future: Challenges for the Next Decade

- Managing systemic risk in global software supply chains
- Securing critical infrastructure against pre-positioning
- Governing offensive cyber operations among major powers
- AI-generated and AI-assisted attacks
- **Talent and workforce shortages**
- Blending cyber with kinetic conflict

Thanks!

areddie@berkeley.edu; brsl.berkeley.edu; @areddie89

Why are we here?

- Will artificial intelligence technologies revolutionize warfare?
- Can the threat of cyber attacks be used to deter adversaries?
- How do governments drive technological innovation in support of national security?
- What is the responsibility of the private sector when engaging in R&D with dual-use applications?

We have lots of questions…

Why are we here?

- Will artificial intelligence technologies revolutionize warfare?
- Can the threat of cyber attacks be used to deter adversaries?
- How should we manage risks from new domains of state competition?
- How do governments drive technological innovation in support of national security?
- What is the responsibility of the private sector when engaging in R&D with dual-use applications?

We have lots of questions…

And few answers…