GAME THEORY APPROACHES TO UNDERSTANDING FUTURE STRATEGIES OF CYBER THREAT ACTORS

Gordon Woo

24th July, 2019

Harvard Business Review

STRATEGY

Games Can Make You a Better Strategist

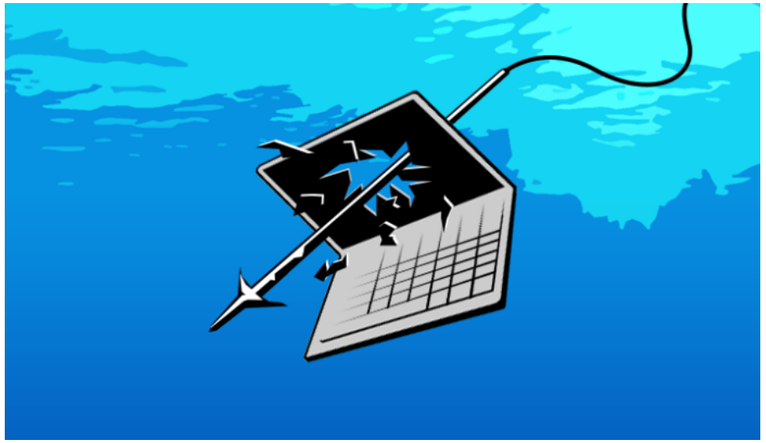
by Martin Reeves and Georg Wittenburg

SEPTEMBER 07, 2015

Games can create an experiential, interactive, and tailored understanding of strategy at low cost and in a scalable manner.

THE NASH EQUILIBRIUM

This is a stable state involving the interaction of different players,
in which no player can gain by a unilateral change of strategy
- if the strategies of the others remain unchanged.



Users' strategies constitute a social optimum if they minimize the sum of the users' losses.

A Nash equilibrium offers a credible prediction of the insider's moves because it gives the insider the best outcome given the defender's strategy.

THE STRATEGIC INTERNATIONAL BLAME GAME

Consider a game consisting of two players: attacker **A** and defender **B**.
A decides whether to attack **B**.

A may or may not be vulnerable to cyber counterattack from **B**;
or political exposure to blame as the cyber attacker.

B may not know whether **A** is vulnerable or not,
or cannot attribute an attack to **A**.

Nash Equilibria exist for the blame game.
A no-attack equilibrium exists only when **A** is vulnerable.

Edwards et al. (2017)

PRACTICAL INSIGHTS FROM GAME THEORY

- Partial tightening of security against specific cyber attack modes will encourage an attacking shift to vulnerable targets, with a higher expected payoff.
- Collective tightening of security against specific cyber attack modes will encourage an attacking shift to other modes, with a higher expected payoff.
- For a given allocation of defensive resources, an attacker will aim to achieve its payoff with the least amount of effort.

PRINCIPAL HACKER MOTIVATIONS

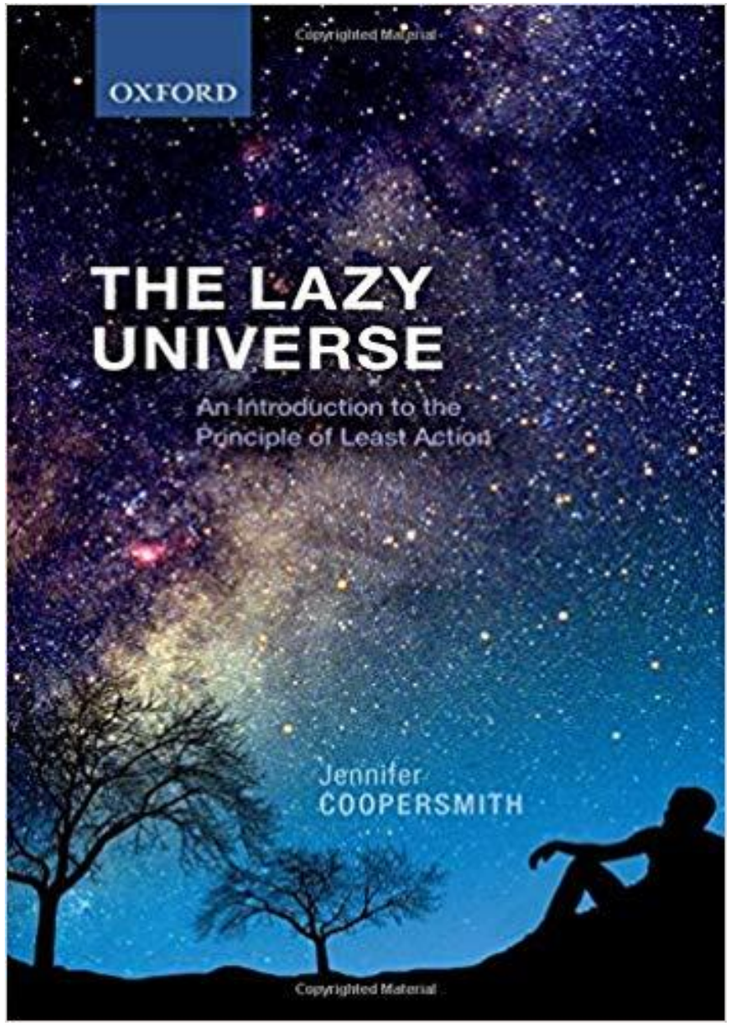
- **Financial gain:** Hackers want the most amount of money they can get for the amount of effort they put in. Targeting small businesses that have lax security can result in a successful attack without much work for the hacker. It can be more lucrative to target multiple soft targets than a hard target.
- **Espionage:** Hackers leverage corporate and government secrets for gain. 90% are associated with state-affiliated hacking groups. Important political objectives warrant the allocation of commensurate resources to commercial espionage, and spying.
- **FIG (Fun, Ideology and Grudge):** Hacktivism, cyber vandalism, cyber terrorism; revenge, disgruntlement.

Calyptix security, July 11, 2017

THE UNIVERSAL PRINCIPLE OF LEAST ACTION

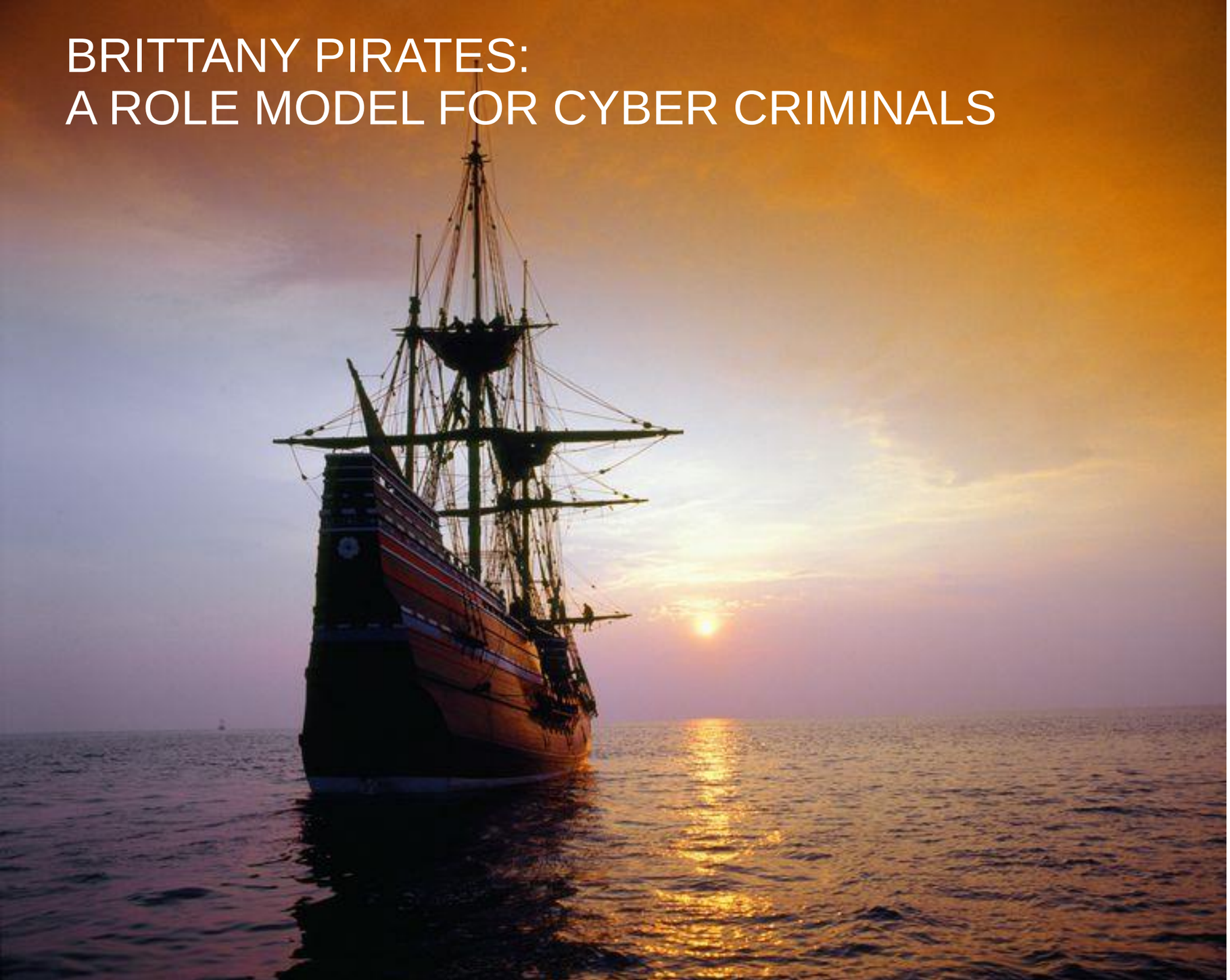
'The great principle is that, in producing its effects, Nature acts always according to the simplest paths.'

Pierre de Maupertuis, 1746



The principle of least action applies to criminal activity.....

BRITTANY PIRATES:
A ROLE MODEL FOR CYBER CRIMINALS



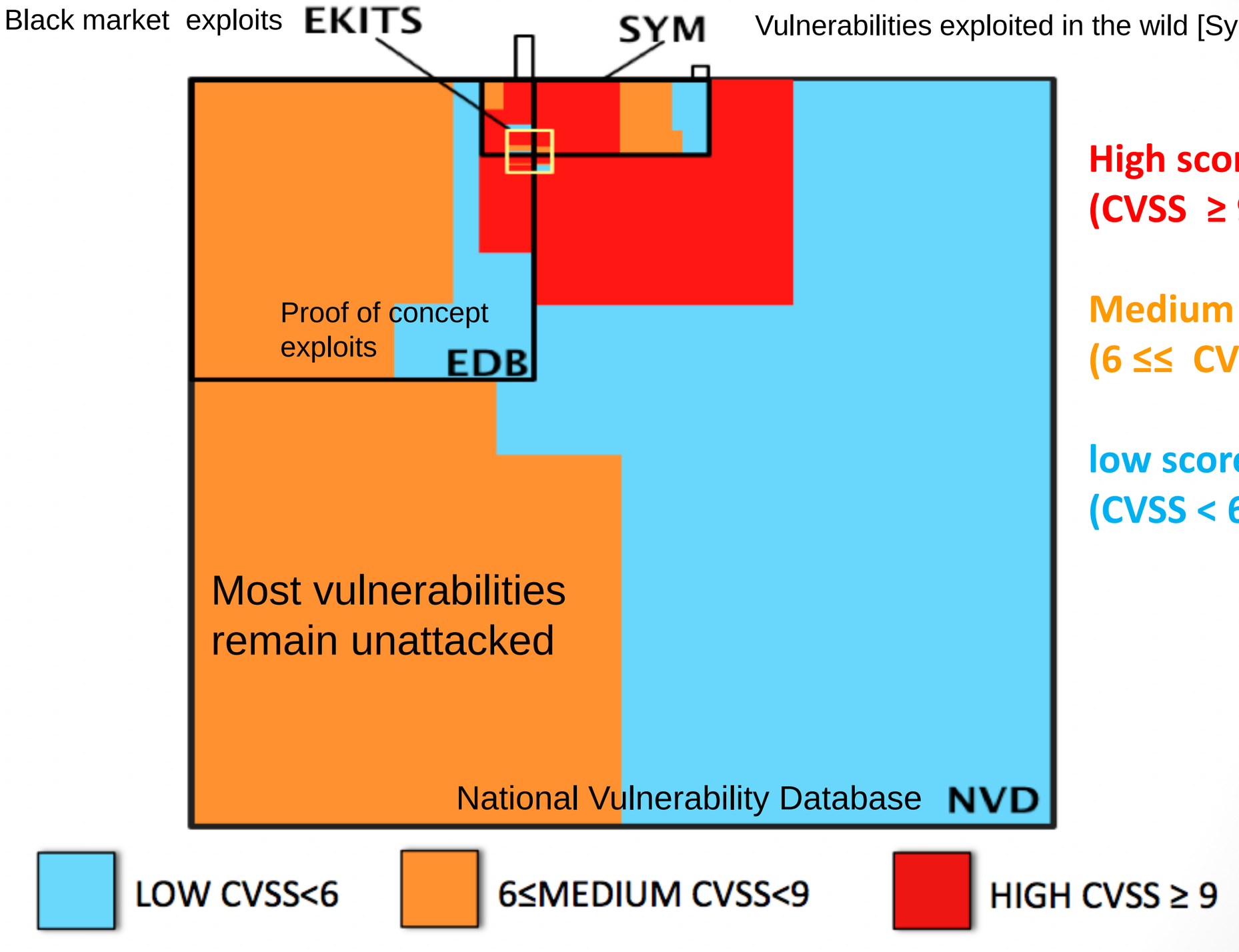
Pierre de Maupertuis' father René was a Brittany corsair.

The 18th century equivalent of a state-sponsored hacker,

he could plunder with no fear of arrest, with booty auctioned off.

THE WORK-AVERSE CYBER CRIMINAL

- Criminals have limited resources, and will aim to attain their objectives with a minimal amount of effort.
- As with terrorists, cyber criminals may opt for off-the-shelf weapons, including those provided by nation states. This enables them to overcome the logistical burden of advanced weapon development.
- A mass cyber attacker will optimally choose whether to weaponize a new vulnerability, or keep using existing toolkits if there are enough vulnerable users.
- Mass cyber attackers may exploit only one vulnerability per software version, and include only vulnerabilities with low attack complexity. They may be slow at introducing new vulnerabilities into their arsenals.



High score vulnerabilities with (CVSS ≥ 9) are in red;

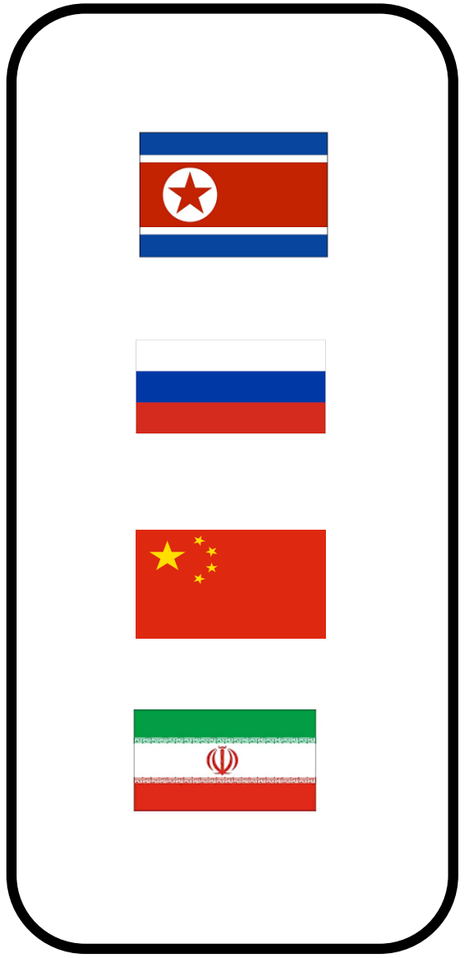
Medium score vulnerabilities with (6 ≤≤ CVSS < 9) are in orange;

low score vulnerabilities with (CVSS < 6) are in cyan.

(Allodi & Massacci, 2013)

Common **V**ulnerability **S**coring **S**ystem

PARASITIC DEPENDENCE ON NATION STATES



New potent cyber weapon

Western Alliance Political & Economic Targets

Cyber Criminals

Adapted cyber weapon
overcoming logistical burden hurdle

Extended range of corporate targets

OPPORTUNIST CRIMINAL USE OF STATE WEAPONS

- As with military weapons, the most powerful cyber weapons are acquired for the arsenals of nation states.
- If they are deployed, leaked or stolen, criminal advantage will be taken to use them or their variants, copying the design philosophy.
- For example, one technique found in conventional criminal malware was inspired by the discovery of Stuxnet. It installed fake device drivers using digital security certificates stolen from two Taiwanese computer component companies, allowing them to evade security software.

DOWNWARD COUNTERFACTUAL GAME

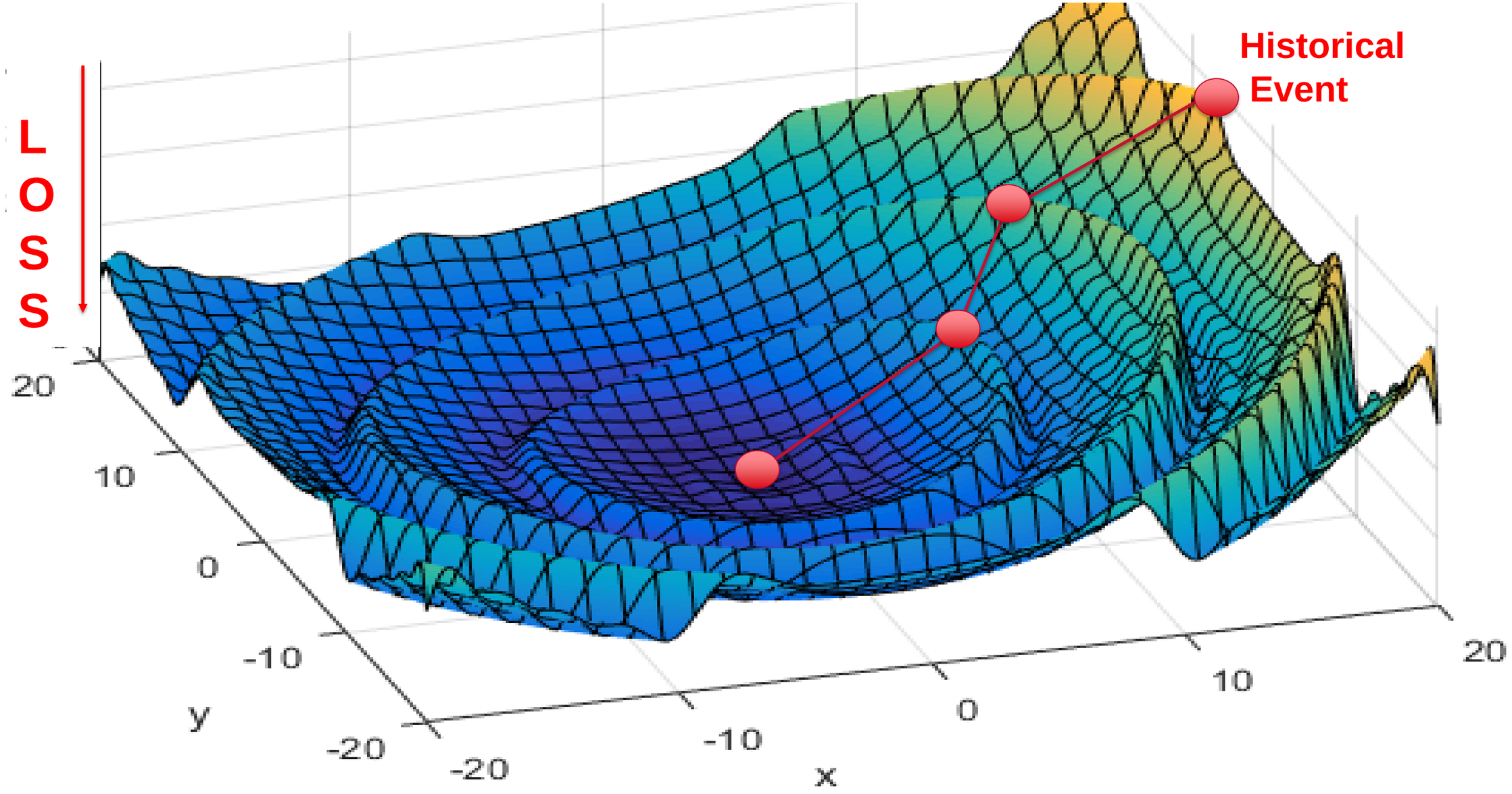
Consider a historical cyber system attack state **S[0]** that led to a major economic loss of **L**.

Construct an alternative cyber system attack state **S[k]** that would have led to a greater economic loss of **L + k* Δ*L**, where **Δ = 10%** , and **k = 1.**

Repeat for ever increasing integer values of **k = 0, 1, 2,….n**

The attacker's challenge: How can S[n] be attained with least effort?

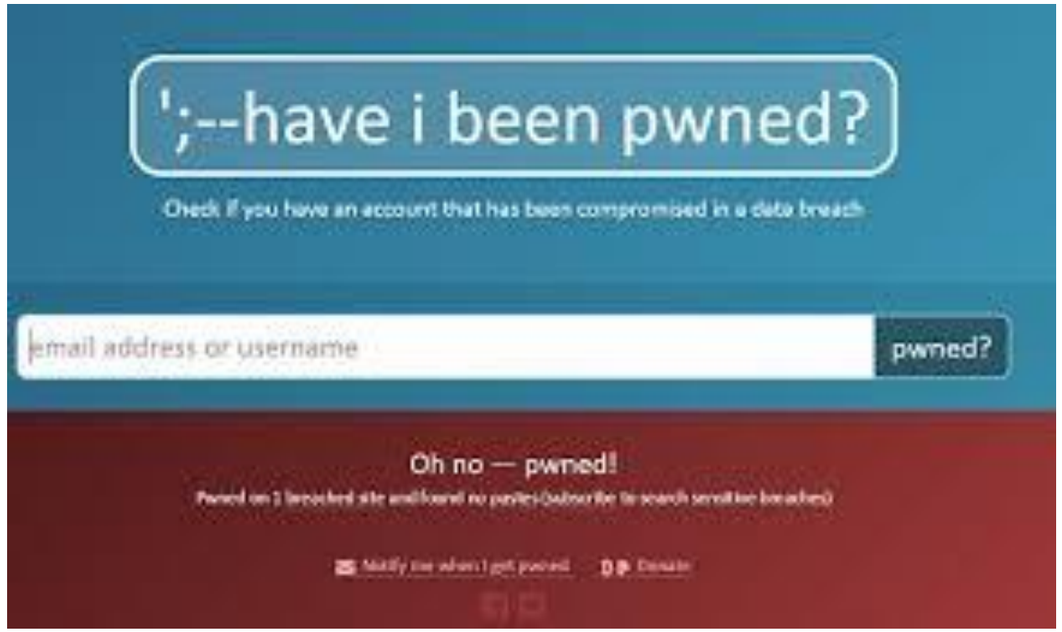
EXPLORING DOWNWARD COUNTERFACTUAL PATHS TO PROGRESSIVELY GREATER LOSS

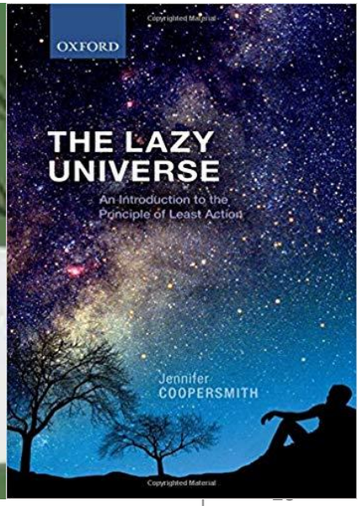


LEAST EFFORT IN SECURITY

Pwned Passwords are **half a billion** real world passwords previously exposed in data breaches.

This exposure makes them unsuitable for ongoing use as they are at much greater risk of being used to take over other accounts.





INCREASING GAIN WITH LEAST MARGINAL EFFORT

Past Cyber Attack State
e.g. state-sponsored

{ X(1), X(2),....X(n)}

Exfiltration of data and money
can be replaced by data deletion
and entire networks being taken down.

Path of least effort

Greater
Loss


Backdoor
shift
http://www.computerhope.com

GAME THEORY INSIGHTS INTO TERRORISM

- Terrorists follow the path of least resistance, and substitute soft targets for well-defended hard targets.
- Terrorists minimize plot size because the interdiction likelihood increases with the number of operatives.
- Sophisticated weapons might be procurable, but not practically developed.

THE CYBER TERRORISM GAME

- Cyber attacks are attractive because otherwise hard physical targets might be vulnerable, and an attack can be launched outside the jurisdiction of the target.
- Terrorism is the language of being noticed: terrorist attacks that kill generate the most international publicity.
- Autonomous transport (road vehicles, ships, drones, helicopters and planes) will increasingly attract the attention of terrorists. [ISIS were known to be interested].
- A Boeing 787 carries more than 10 million lines of code. The more complex the software, the more likely it will be that cyber terrorists will seek to expose flaws.

A productive and efficient strategy for cyber threat actors is to seek to achieve their desired payoff with minimal marginal effort.

This strategy yields high attack leverage: payoff / effort.