ACTIVE DEFENSE & THE A.R.T OF W.A.R.

Lessons in *offensive* resilience taken from the evolution of modern mixed martial arts

@beaker


AMERICA HAS LOST ITS FIRST CYBERWAR
No one should kid themselves. With the Sony collapse America has lost its first cyberwar. This is a very, very dangerous precedent.
#CyberwarOnAmerica

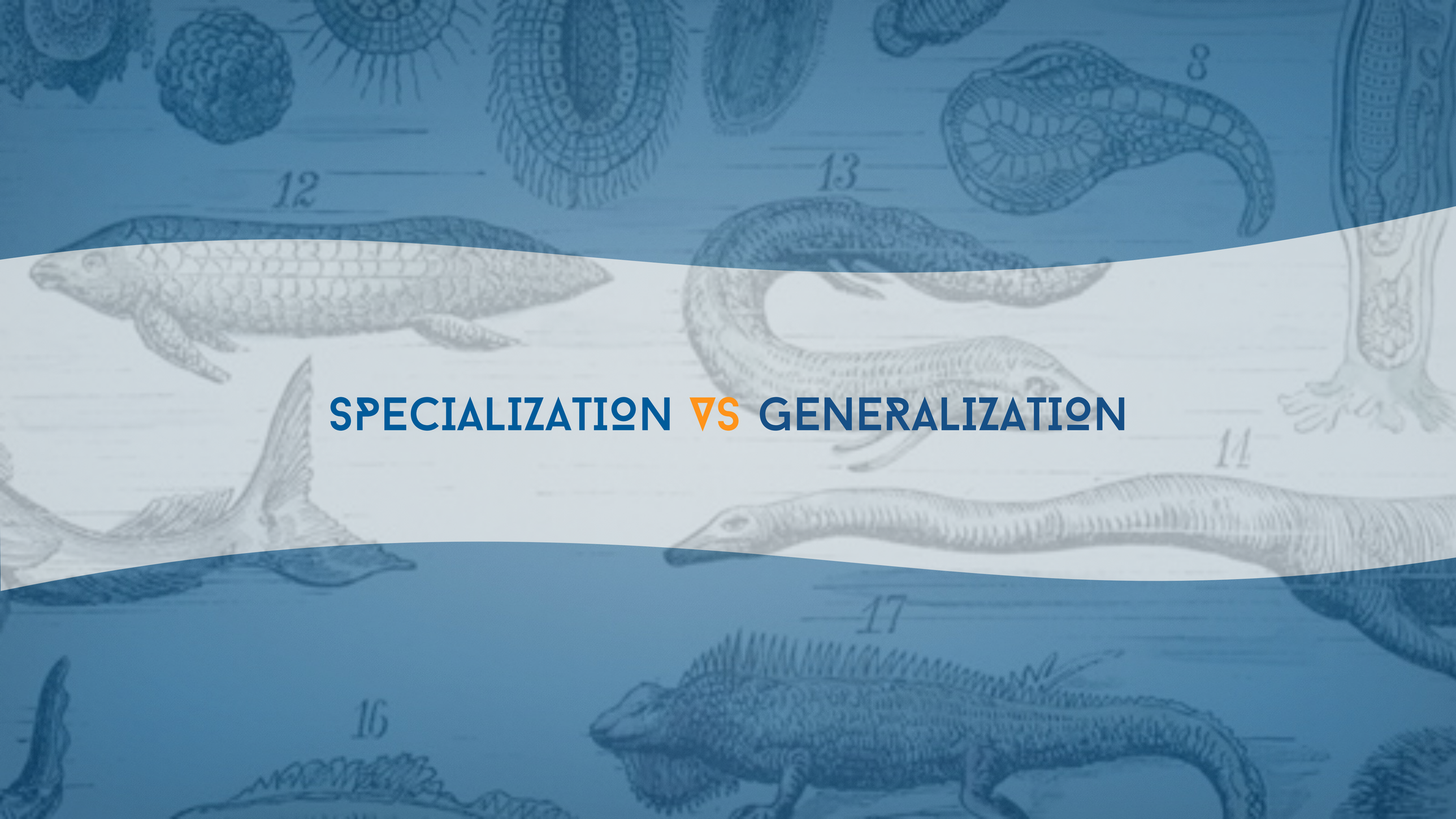
SECURITY SPECIALIZATION VS GENERALIZATION

BY WAY OF THE EVOLUTION OF MIXED MARTIAL ARTS

ACTIVE DEFENSE
"OFFENSIVE" RESILIENCE

THE A.R.T. OF W.A.R.

ACTIVE RESPONSE TECHNIQUES OF WEAPONIZATION AND RESILIENCE



SPECIALIZATION VS GENERALIZATION

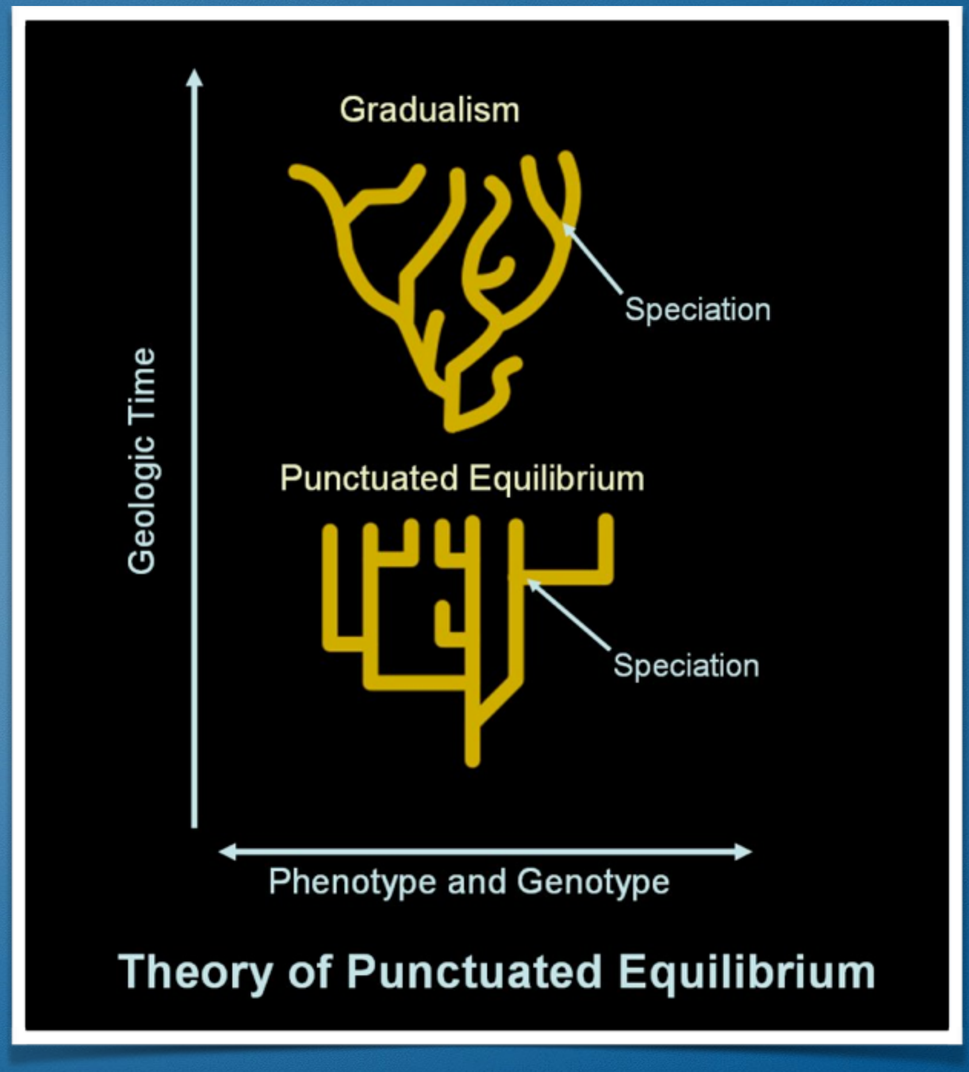
Darwin, Evolution, Adaptation and the Theory of Punctuated Equilibrium*

Darwin's theory of evolutionary selection posits that variation within species occurs randomly and that the survival or extinction of each organism is determined by that organism's ability to adapt to its environment; this is known as *"natural selection."* Adaptation is also related to how specialized a species is.

There are two theories describing biological evolution:

Gradualism: evolution generally occurs uniformly and by the steady and gradual transformation of whole lineages and is seen as smooth and continuous.

Punctuated equilibrium: most species will exhibit little net evolutionary change for most of their geological history, remaining in an extended state called stasis. When significant evolutionary change occurs, it is generally restricted to rare and rapid events of branching speciation by which a species splits into two distinct species, rather than one species gradually transforming into another.



*http://en.wikipedia.org/wiki/Punctuated_equilibrium

ADAPTATION AND EVOLUTION

The “next generation” of fighters ARE *Mixed* Martial Artists







Evolutionary Speciation in Security

The scale of measured evolution in Security is tiny, but it lends itself to the T.O.P.E. driven by technological and adversarial disruption

Infostructure — Content & Context - Data & Information

Applistructure — Apps & Widgets - Applications & Services

Metastructure — Glue & Guts - IPAM, IAM, BGP, DNS, SSL, PKI & Abstraction layers

Infrastructure — Sprockets & Moving Parts - Compute, Network, Storage

→ **Information Security**

→ **Application Security**

→ **Network Security**
Host-based Security
Storage Security

Scale, Virtualization, Automation, APIs & DevOps: Adaptation

Nobody messes with A BLOWFISH

ACTIVE DEFENSE & ACTIVE RESPONSE

WHEN DOES DEFENSE STOP & OFFENSE BEGIN?

It's a matter of perspective, intent, initiation and outcome...

DEFINING "ACTIVE DEFENSE"

I'm so glad we all agree…

Rich Mogull, Securosis:

"Altering your environment and system responses dynamically based on the activity of potential attackers, to both frustrate attacks and more definitively identify actual attacks. Try to tie up the attacker and gain more information on them without engaging in offensive attacks yourself."

Joint Education and Doctrine Division, U.S. Department of Defense:

"The employment of limited offensive action and counterattacks to deny contested area or position to the enemy."

Dave Dittrich, University of Washington:

"The term active defense, while a popular phrase, is problematic from many perspectives. It combines the terms active (meaning to engage, as opposed to its antonym passive) and the term defense (implying defending from or reacting to an attack)…Advocates who use language suggesting striking or fighting back when attacked further confuse the issue and degrade the utility of this term (see also Retribution)."

DEFINING "ACTIVE RESPONSE* TECHNIQUES"

"**The Active Response Continuum** comprises a variety of different tactics for responding to unauthorized digital intrusions…[including] a variety of reactive, non-cooperative responses to digital intrusion that are typically calculated to affect remote systems and are intended to investigate, defend, repel, or punish the intrusion. Such measures range from benign measures that implicate the legitimate interests of innocent persons without impacting remote systems to aggressive measures that are intended to inflict harm or damage on the intended targets."

*Active Response to Computer Intrusions - 2005 Dave Dittrich & Kenneth Einar Himma, Ph.D., J.D. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=790585

INTRUSION RESPONSE & LEVELS OF FORCE

Levels of Intrusion Response		
Level	**Victim Posture**	**Characteristic Actions**
0	Unaware	None: Passive reliance on inherent software capabilities
1	Involved	Uses and maintain anti-virus software and personal firewalls
2	Interactive	Modifies software and hardware in response to detected threats
3	Cooperative	Implements joint tracebacks with other affected parties
4	Non-Cooperative (Active Response)	Invasive tracebacks, cease-and-desist measure and retaliatory counterstrikes

Levels of Force		
Level	**Causal Impacts**	**Characteristic Actions**
Benign	Limited to victim's own systems	Sniffing, scanning, readdressing hosts, honeypots
Intermediate	Impacts on remote systems but not calculated to produce damage	Invasive tracebacks, remote evidence collection
Aggressive	Impacts calculated to produce damage in remote systems	Remote exploitation, corruption of data, denial of service

"2015 IS THE YEAR OF OFFENSIVE DECEPTIONS"

Gartner.

WHY GARTNER | ANALYSTS | RESEARCH | EVENTS | CONSULTING | ABOUT

Lawrence Pingree

A MEMBER OF THE GARTNER BLOG NETWORK

« Back to GBN Home

Lawrence Pingree
Research Director
2 years with Gartner
16 years IT industry

Lawrence Pingree's responsibilities include coverage of security technologies and the cloud security space. His main focus is on conducting research targeted at the security aspects of products in the data center… Read Full Bio

Coverage Areas:

← Conflict of interest or not?
Top 5 things AR professionals should consider when doing a Vendor Briefing →

2015 is the year of Offensive Deceptions

by **Lawrence Pingree** | December 23, 2014 | 1 Comment

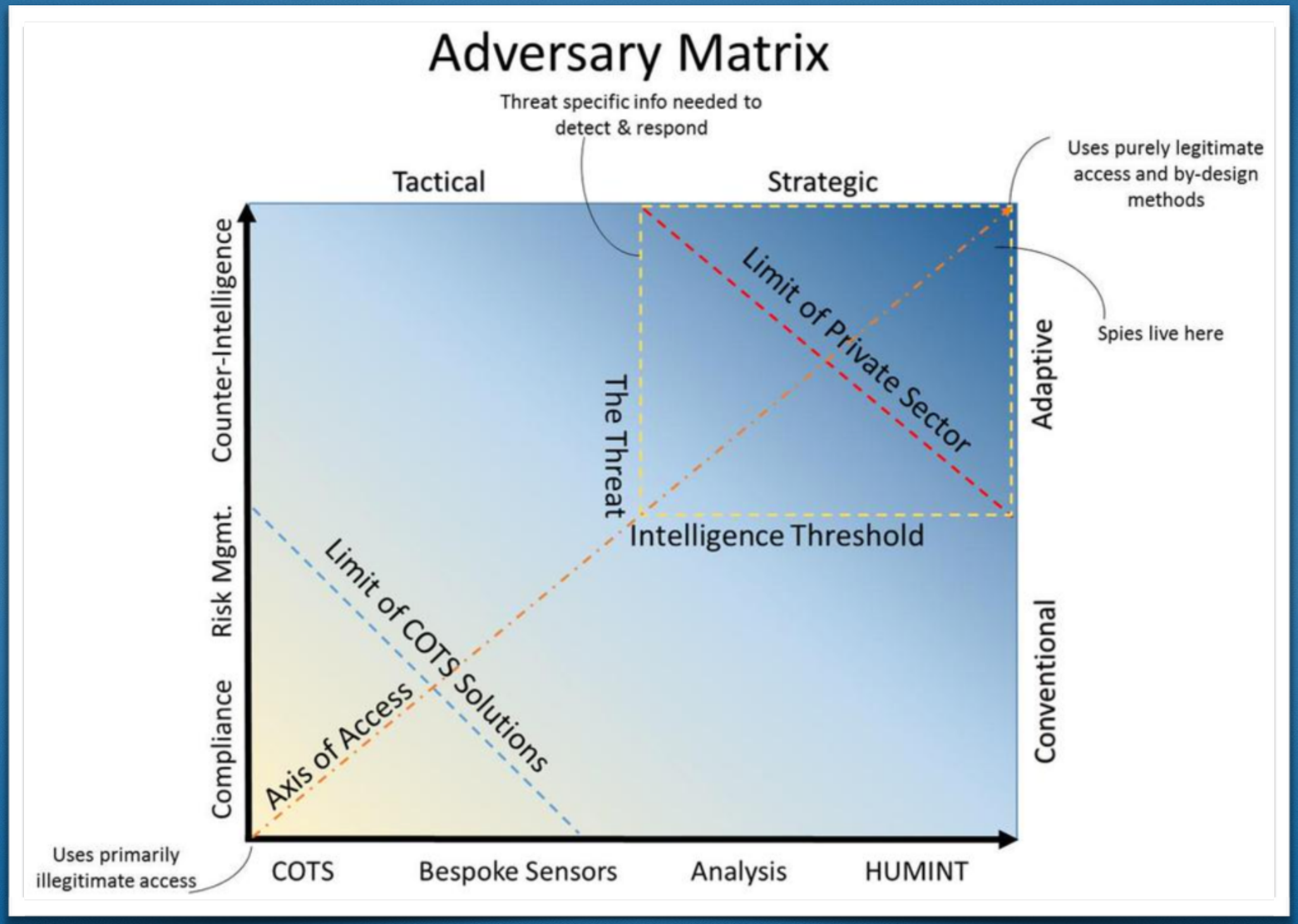
During the past, security technologies have largely focused on detection and blocking mechanisms to respond to attacks. Security of course must continuously evolve to detect and defend against attacker strategies, and these past strategies must continue to include new capabilities as well as old to properly defend against the array of attack techniques. A new emerging technology response capability is to "deceive" as a response.

The future of security will incorporate defense in depth, detection in depth, contextually aware adaptive response and increasingly leverage offensive misdirection and deception techniques with the goal of overwhelming and delaying attacker activities. Providers of deception and misdirection techniques are emerging while these same capabilities in some existing security products. Using attacker deceptions as a response strategy will have a game-changing effect on hacker attack campaigns.

"The future of security will incorporate defense in depth, detection in depth, contextually aware adaptive response and *increasingly leverage offensive misdirection and deception techniques with the goal of overwhelming and delaying attacker activities.* Providers of deception and misdirection techniques are emerging while these same capabilities in some existing security products. Using attacker deceptions as a response strategy will have a game-changing effect on hacker attack campaigns."

THE A.R.T. OF WEAPONIZATION AND RESILIENCE (W.A.R.)

THREAT MODELS MATTER



John Lambert - General Manager, Microsoft Threat Intelligence Center

HOT

OR

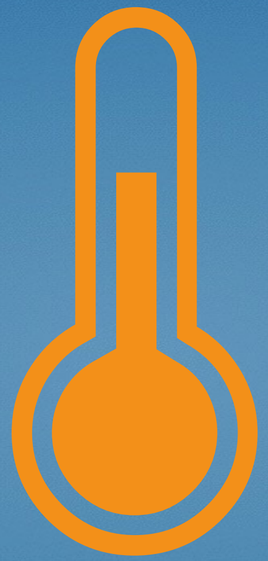
NOT?

LET'S GAUGE OUR TOLERANCE…

1. High Interaction Honeypots that leverage deception, evasion and fake data

2. Active Web bugs/beacons in docs that phone home for attribution/tracing of IP exfiltration

3. Implanting/seeding fake hash-compatible files in P2P networks to corrupt content distribution



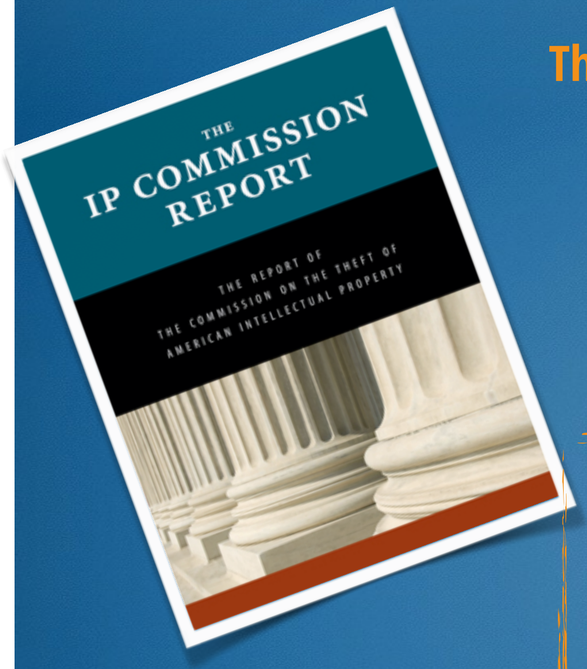
4. Packet reflection and/or Targeted App-level DoS against attackers actively targeting assets

5. ISPs providing automatic quarantine and remediation of malware on subscriber assets

6. Implant malware in attempted-exfiltration data to degrade/delay/damage/ destroy

…FOR WEAPONIZATION & RESILIENCE

THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY MAY 22, 2013



The Commission recommends the following measures to address cybersecurity:

1. Implement prudent vulnerability-mitigation measures.

This recommendation provides a summary of the security activities that ought to be undertaken by companies. Activities such as network surveillance, sequestering of critical information, and the use of redundant firewalls are proven and effective vulnerability-mitigation measures.

2. Support American companies and technology that can both identify and recover IP stolen through cyber means.

Without damaging the intruder's own network, companies that experience cyber theft ought to be able to retrieve their electronic files or prevent the exploitation of their stolen information.

3. Reconcile necessary changes in the law with a changing technical environment.

Both technology and law must be developed to implement a range of more aggressive measures that identify and penalize illegal intruders into proprietary networks, but do not cause damage to third parties. Only when the danger of hacking into a company's network and exfiltrating trade secrets exceeds the rewards will such theft be reduced from a threat to a nuisance.

http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf

CONDITIONAL COUNTERSTRIKES?

Jan Kallberg, Cyber Security Research and Education Institute

"If corporate entities were allowed to hack back and engage foreign entities in cyberattack exchanges, according to the model proposed by the Commission on the Theft of American Intellectual Property, it relies on several assumptions.

These assumptions are also present in other propositions of allowing corporations to hack back, as the assumptions are general, and underlying the general argument:

1. The private companies can attribute
2. The counterstriking corporations have the ability to engage a state sponsored organization.
3. The will be no uncontrolled escalation.
4. The whole engagement is locked in between parties A and B with sufficient ability to created an encapsuled deterrence by the initial defender
5. The initial attacker has no second strike option
6. The counterstriking company has no interests or assets in the initial attacker's jurisdiction
7. The duplicated intellectual property is at one location


Kallberg, Jan, "A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs," IT Professional , vol.17, no.1, pp. Jan.-Feb. 2015
doi: 10.1109/MITP.2015.1

A Right to Cyber Counter Strikes
The Risks of Legalizing Hack Back

Jan Kallberg
Cyber Security Research and Education Institute
Erik Jonsson School of Engineering and Computer Science
The University of Texas at Dallas
Richardson, TX 75083-0688
jkallberg@utdallas.edu

The idea to legalize hacking back has gained traction the last years and received several influential corporate and political proponents in the United States and Europe. The frustration with repeated cyberattacks and lack of credible law enforcement pushes for alternative ways to prevent future cyberattacks. As of today, counter cyberattacks are illegal in a majority of the nations because it constitutes another cybercrime independent from the initial attack. If cyber counter strikes were legalized it relies a set of questions. The first line of questions are linked to the underlying assumptions that the attacker can be identified, located and attacked challenges upon. The second line of questions are the embedded challenges to the rule of the nation state. Privately executed counter cyberattacks would undermine the authority and legality of the state. The questions raised by legalizing hack back of cyberattacks would have a negative impact on the development of Internet governance and norms.

Keywords – cyber security, cyber defense, retaliation, cyber deterrence, cyber ethics, hack back, intellectual property, cyber theft

I. INTRODUCTION

In the recent years there have seen several vocal proponents for legalizing corporations to hack back after being targeted by a cyber-attack. As of today, the act of hacking back constitute an illegal actions as there is not a legal right to digital self-defense, instead a counterattack is a new perpetrated attack [1, 2].

A strong proponent is the United States has been the Commission on the Theft of American Intellectual Property, a bipartisan commission [3]. The focus for the discussions in the United States has been centered on corporate interests, and the potential loss of intellectual property derived from successful cyberattacks [4, 5]. The Netherlands, Finnland, and the United Kingdom have had similar debates about the future legalization of hacking back. The rationale in Europe has been from a law enforcement stand point instead from a strict corporate outlook. In a European perspective hacking back would allow law enforcement to conduct investigations by hacking into cybercriminal computers and networks. The unknown is if hacking back is a viable route to address the problem or if hacking back would trigger new problems and challenges that could lead an entropy in Internet governance and instead delay a formation of regulating cyber norms codified by national legislators and international organizations. Multinational governmental entities such as the United Nations (UN), the International Telecommunications Union (ITU), the European Union (EU), the Internet Corporation for Assigned Names and Numbers (ICANN), work together with national legislators and Internet groups to create norms and rules for the Internet and the future utilization of the net. If corporations have a broad mandate to strike back against backers it is likely dissolving Internet public norms because the driving force is then the best interest of the corporation at the point of corporate decision making. The idea with public Internet norms is to balance private and public interests.

The main question raised in this paper is if legalization of corporate hack back is a viable route – or if the approach is based on weak assumptions. The report from the Commission on the Theft of American Intellectual Property is a central document, due to its acceptance within the corporate and political sphere, and the report advocates hacking back to recover stolen intellectual property and data.

II. GROWING FRUSTRATION

The last decades have seen a shift from cyber criminals to foreign entities [6,7], and increasingly state actors, seeking to gain a geopolitical, military, industrial, competitive, intelligence or commercial advantage. The state actors have access to a variety of options that the earlier cyber criminals did not possess, such as integration to intelligence community, government aligned business interests, and the state sponsored attack were well funded with more resources allocated. The entity of state sponsored attack have increased the targeted states' concerns, even if the targeted states' bureaucracy themselves are not affected but instead their business and society. In an effort to address this new threat, the nation states have pursued cyberdefense abilities.

Several advanced democracies, and their ministries of defense are creating what they define as cyber warfare units. The question is if these fairly small military cyber defense units will have an impact in a cyber-conflict as these units are to a high degree forensic team seeking attribution and

http://works.bepress.com/cgi/viewcontent.cgi?article=1053&context=jan_kallberg

WHY CALLING EVERYTHING "CYBERWAR" IS PRICKLY

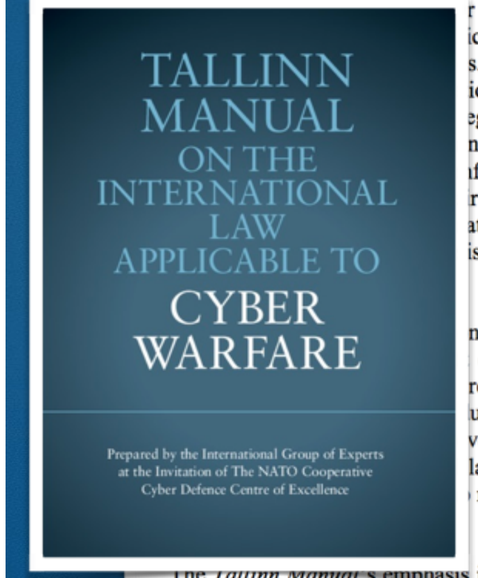
Scope

The *Tallinn Manual* examines the international law governing 'c
general matter, it encompasses both the *jus ad bellum*, the internati
resort to force by States as an instrument of their national policy, a
international law regulating the conduct of armed conflict (also la
the law of armed conflict, or international humanitarian law)
international law, such as the law of State responsibility and the la
within the context of these topics.

Cyber activities that occur below the level of a 'use of force' (as
r criminality, have not been addres
ic cyber actions, except with regard
s. For instance, the Manual is wit
ional law, such as internation
egality of cyber intelligence activit
notions of 'use of force' and 'arme
nflict governed by the *jus in bello*
r jurisdiction must comply with a
ations have likewise not been co
issue of individual criminal liabilit

n 'cyber security' as that term is
of intellectual property, and a w
real and serious threats to all
uals. An adequate response to ther
ver, the Manual does not address
law on uses of force and armed co
more applicable to these threats in

The *Tallinn Manual*'s emphasis is on cyber-to-cyber operations, *s*
include the launch of a cyber operation against a State' critical in
attack targeting enemy command and control systems. The Man
use in considering the legal issues surrounding kinetic-to-cyber
aerial attack employing bombs against a cyber control centre.
address traditional electronic warfare attacks, like jamming. These
well understood under the law of armed conflict.



Computer Fraud & Abuse Act

Computer Fraud and Abuse Act (18 USC 1030)

COMPUTER FRAUD AND ABUSE STATUTE

' 1030. Fraud and related activity in connection with computers

(a) Whoever

(1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer,

(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

shall be punished as provided in subsection (c) of this section.

(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby

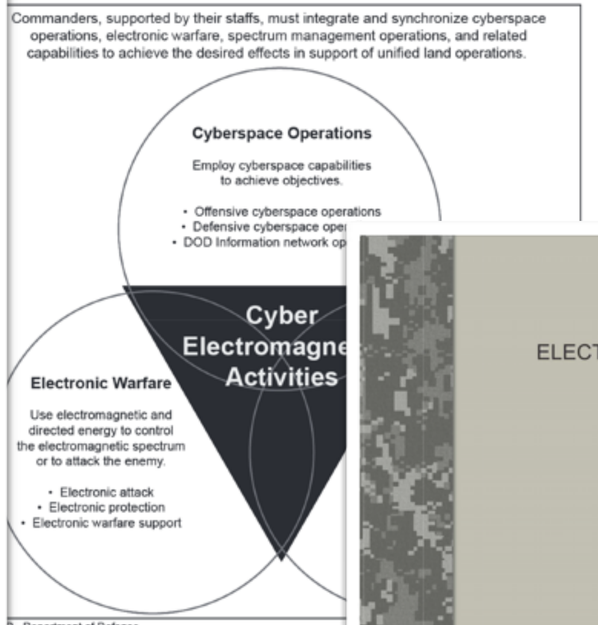
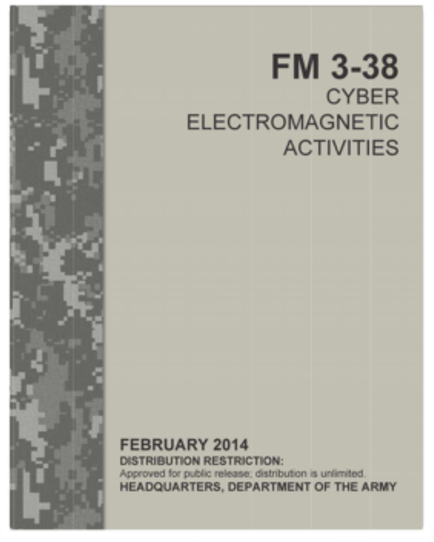


Figure 1-1. Cyber electromagne

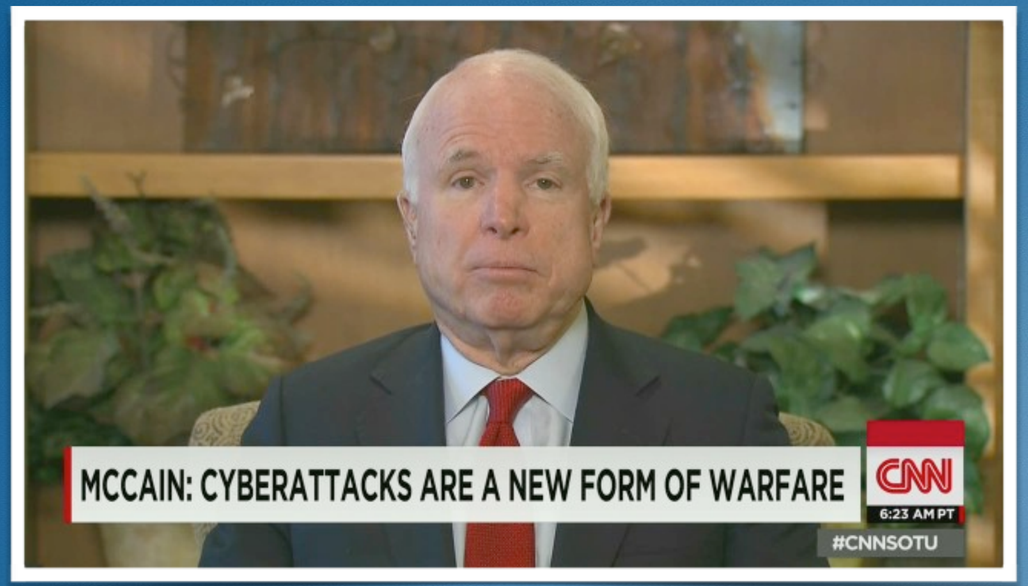
Army forces conduct CEMA as a unified effort. *Integra*
r actions to create a force that operates by engaging as
ngement of military actions in time, space, and purpose to
cisive place and time (JP 1-02). CEMA integrates and sy
EW, and SMO to produce complementary and reinf
pendently may detract from their efficient employment. If
flicts and mutual interference between them and with other entities that use the electromagnetic
trum (EMS). CO, EW, and SMO are synchronized to cause specific effects at decisive points to
port the overall operation.

The CEMA element is responsible for planning, integrating, and synchronizing CO, EW, and SMO
upport the commander's mission and desired end state within cyberspace and the EMS. During
cution the CEMA element is responsible for synchronizing CEMA to best facilitate mission
mplishment. (See chapter 2 for more information on the CEMA element.)

FM 3-38 12 February 2014



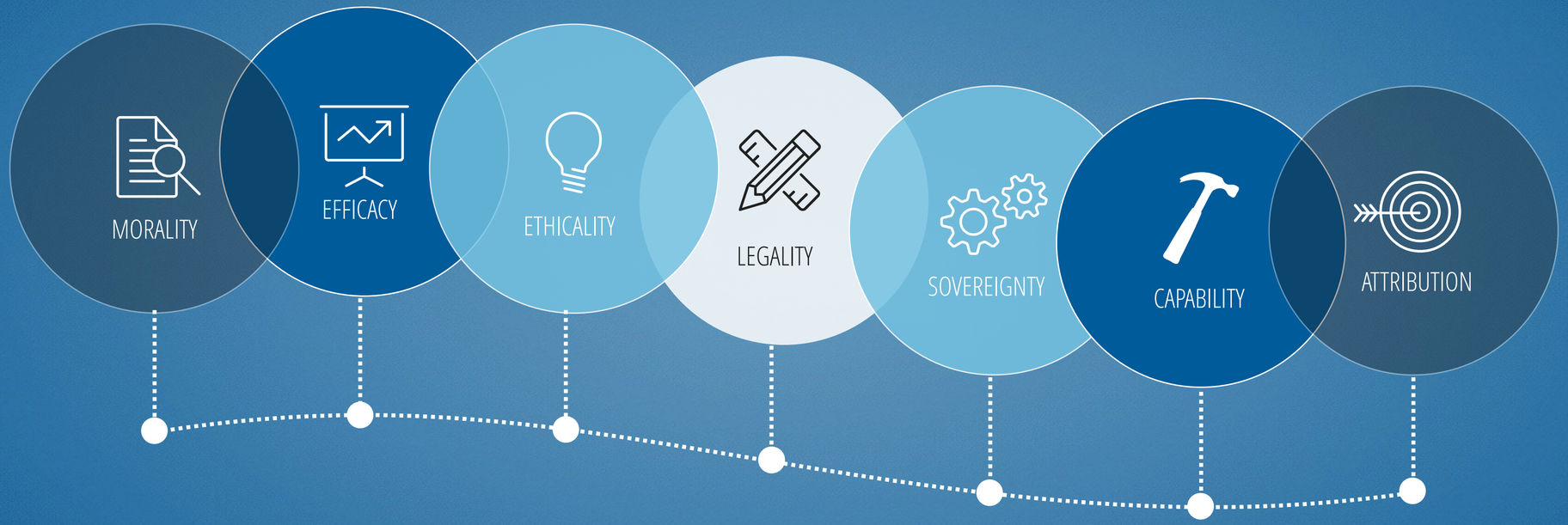
PRECISION MATTERS




“I’ll call it Cyberwar when you can get a purple heart for carpal tunnel syndrome”
-@swiftonsecurity

A SLIPPERY SLOPE

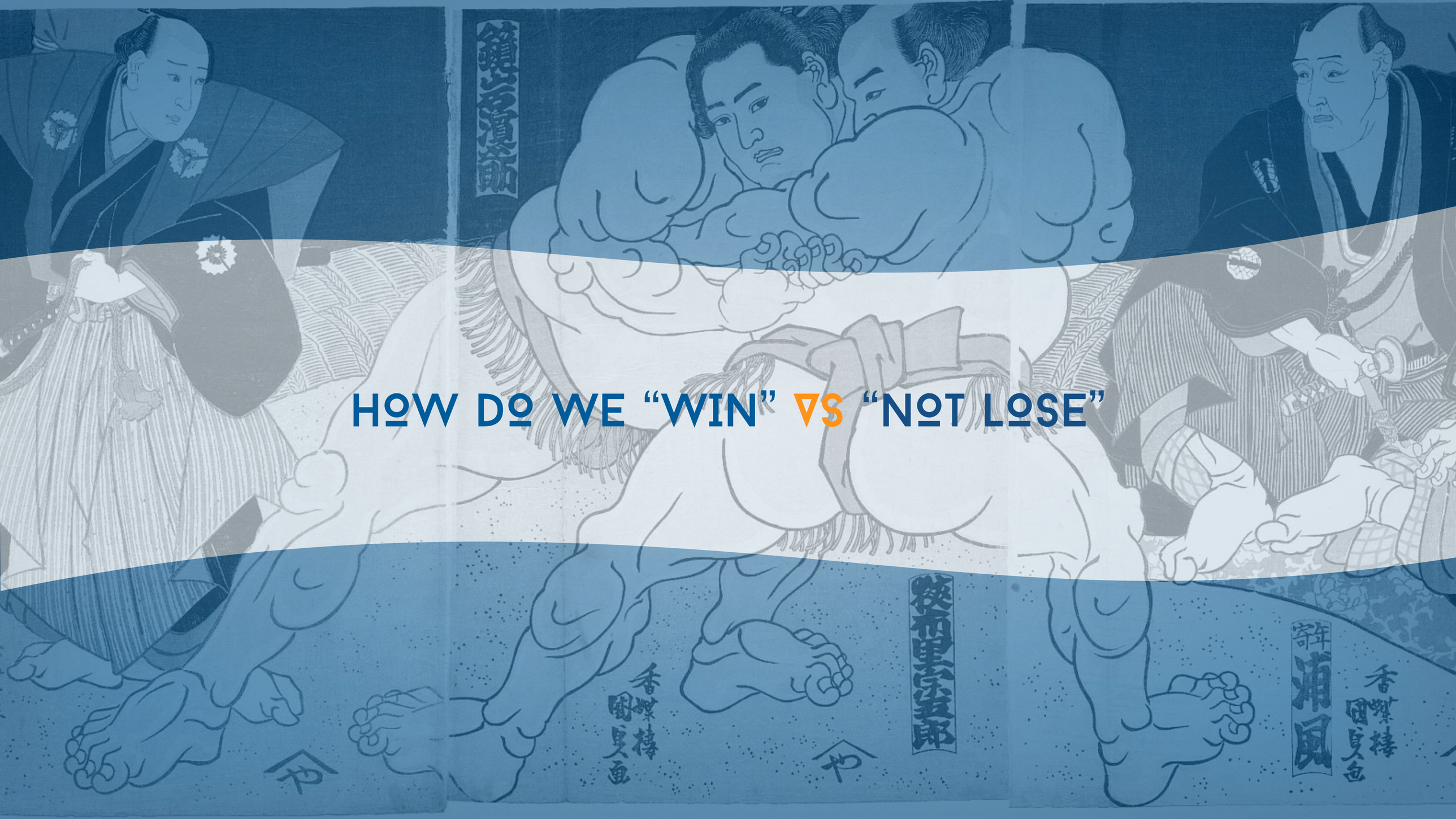
Many things to consider beyond technology…



ATTRIBUTION IS HARD

— SAID SOMEBODY, ONCE.

OK, IT WAS ME...
BUT YOU CAN'T PROVE IT.



HOW DO WE “WIN” VS “NOT LOSE”


Nobody messes with
A BLOWFISH

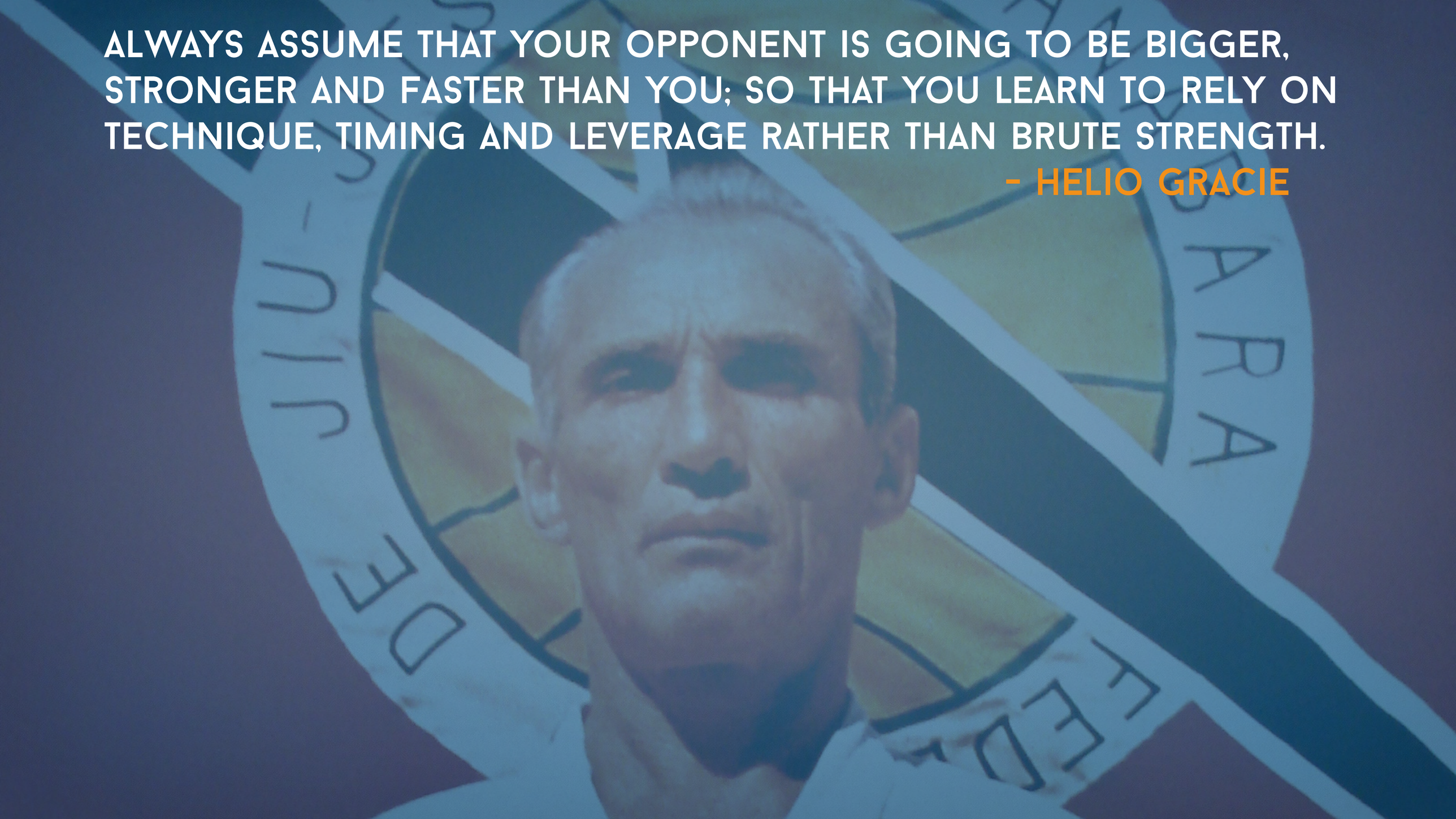
MANAGING ACROSS THE ACTIVE RESPONSE CONTINUUM

1. We need precision in language and context. The issue is that the "rules of engagement," the terms of art and the scope of such are not commonly understood or agreed to…within the security industry, community, or government. Example: conflating vandalism, crime, espionage, terrorism with "war." Our adversaries count on this dissonance

2. Technologically we have the capability to be more aggressive in our defensive posture but we must evolve our capabilities and invest in growing the skill base of our defenders; it is not simply a technology play. We need to grow our next generation of operators with broader skills and enable cross-functional, cross-domain knowledge.

3. We desperately need to utilize better threat modeling, automation, trustable analytics and actionable threat intelligence to defend ourselves "actively," but that also relies upon the ability to make scalable headway with attribution and hand-offs

4. There are things we can do today across the Active Response Continuum that allow us to be more responsive, adaptive and more resilient as we come to terms with the outcomes and impact that attacks are having culturally, economically, and politically. We cannot afford the mindset that we are forever bounded by the capabilities of our adversaries. Forensics and post-breach clean-up is not an effective or sustainable resilience strategy


ALWAYS ASSUME THAT YOUR OPPONENT IS GOING TO BE BIGGER, STRONGER AND FASTER THAN YOU; SO THAT YOU LEARN TO RELY ON TECHNIQUE, TIMING AND LEVERAGE RATHER THAN BRUTE STRENGTH.
- HELIO GRACIE

THANKS

@beaker

www.rationalsurvivability.com

2008

2009

2010

2010

2011

2012

2013