



Thwarting Virtual Jailbreaks

Tom Kellermann, CEO of Strategic Cyber Ventures LLC and Wilson Center Global Fellow

Cyberspace in 2017 – decades after its creation – remains a free-fire zone. A multiplicity of actors, the absence of norms and inadequate cybersecurity standards that fail to mitigate the modern kill chain creates the perfect storm for a simmering online insurgency quickly picking up steam. Sophisticated cyber espionage campaigns carried out by nation states are escalating, from [Pawnstorm](#) to the [MenuPass Group](#). Meanwhile, individuals – for a variety of reasons – are turning toward organized hacktivism.

For the foreseeable future, governments won't – and may not be able to – civilize the new cyberspace,

and this necessitates a defensive paradigm shift. Perimeter security is no longer sufficient. What we need is a cybersecurity architecture that mimics a SuperMax prison.

Doing so requires a deeper understanding of how attackers attack, and what they do once they are inside the castle walls. You have to know your network inside and out.

The new cybersecurity paradigm

As the recent [Verizon Data Breach Report](#) noted, most breaches are not discovered for at least

100 days. According to the same report, 81.9% of compromises are caused by breaches that took minutes to accomplish, while 67.8% of compromises took days to reach the exfiltration stage. It took months for a victim organization to respond to a cyber intrusion.

Given the fact that cyber actors have a footprint within networks for an extended period, organizations must alter their security posture accordingly; the metric by which we should assess the potency of a cyber-countermeasure is how effectively it can decrease an adversary's dwell time.

The importance of early detection is that the more dwell time the adversary has in the environment, the longer it takes to detect and contain a data breach, the more costly it becomes to resolve, and the harder a brand's reputation is hit.

In 1934, the United States Department of Justice opened Alcatraz Prison in San Francisco Bay. The purpose was to incarcerate prisoners that caused trouble at less secure facilities. Many considered it the gold standard.

It closed decades later, and recognizing that there were even more sophisticated ways to house the most dangerous inmates, the Federal Bureau of Prisons opened the Administrative Maximum Facility (ADX) in Florence, Colorado, housing the likes of Ted Kaczynski, Timothy McVeigh, and Robert Hanson.

These SuperMax "control-unit" prisons, or units within prisons, represent the most secure levels of custody. The objective is to prevent prisoners from knowing their specific location within the complex. Among many measures to make escape as difficult as possible, inmates, for example, only see sky

and roof through their windows. The prison as a whole contains motion detectors, cameras, remote-controlled steel doors and pressure pads. While prisons try to keep people in, they also keep people out.

A SuperMax for your Network

The same construct should be applied to today's hybrid network environment. To thwart a virtual jailbreak with your intellectual property and credentials that could cause irreparable damage to a reputation, cybersecurity leaders must embrace the concept of "intrusion suppression" by altering their architecture to emulate the "SuperMax" prison.

Intrusion suppression requires clandestine detection, deception, diversion and eventual containment of a cyber adversary. It involves four steps that aim to detect cybercriminals by decreasing their dwell time and lateral movements:

- Deploy a deception grid (this means deceive and divert the adversary unbeknownst to them) to enhance situational awareness;
- Deploy user entity behavior analytics, which provides contextual analysis on the activity and lateral movement of the adversary;
- Deploy adaptive authentication with contextual verification to eliminate any access an adversary has to your network; and
- Embrace memory augmentation to hunt the adversary in the wild.

These investments are fundamental to turn the tables on the cybercriminal of 2017. Not only will they help keep costs down in the event of a breach by stifling the adversary's exfiltration of meaningful

data, but they will also help protect the reputation of the enterprise that has been breached.

Possible Policy Options

But industry will not turn the tide alone. Governments, specifically led by the US, must consider the following efforts to better police cyberspace and reduce threats:





- **The Department of Justice and the Federal Trade Commission** could update their policy statement on cybersecurity information sharing to state clearly that antitrust laws should not pose a barrier to intra-industry coordination on active defense against cyber threats.
- **The Federal Communications Commission** could increase efforts to tackle distributed denial of service attacks via automatic authorization to sinkholes.
- **The US Congress** could establish a tax credit for business and individuals who make cybersecurity investments.

- **The US Congress** could assess existing constraints on active defense, especially regarding low and medium-risk active defense measures. i.e. [Deception security technologies](#)
- **The US Congress** could review regulation over digital currencies and alternative payments systems that facilitate money laundering associated with cybercrime and cyberespionage. The proceeds of this forfeiture could be allocated to critical infrastructure protection in cyberspace.

Now is the time to spin the chessboard. We must understand our adversaries better – who they are and what they want – and build a structure that inhibits the free movement of the adversary once they penetrate a system.

The opinions expressed in this article are those solely of the author.

The Wilson Center

-  wilsoncenter.org
-  facebook.com/WoodrowWilsonCenter
-  [@TheWilsonCenter](https://twitter.com/TheWilsonCenter)
-  202.691.4000

Digital Futures Program

-  wilsoncenter.org/program/digital-futures-project
-  digitalfutures@wilsoncenter.org
-  facebook.com/WilsonCenterDFP
-  [@WilsonCenterDFP](https://twitter.com/WilsonCenterDFP)
-  202.691.4002



Tom Kellermann

tom.kellermann@wilsoncenter.org

Tom Kellermann is CEO of Strategic Cyber Ventures and a Wilson Center Global Fellow. He was previously Chief Cybersecurity Officer for Trend Micro and has over 19 years of experience in the cybersecurity field.

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027