Cyber

How the Founding Fathers helped make the US cyber-resilient

By **Jan Kallberg**

Apr 18, 2019

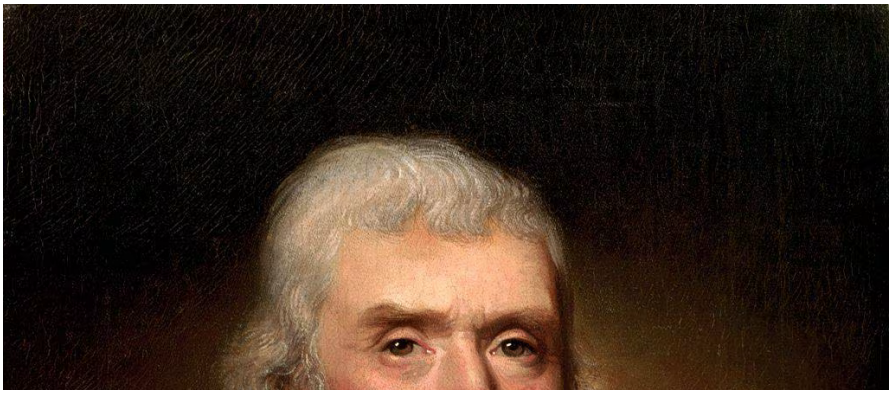
Featured Video

Honoring accomplishment and courage: profiles of the 2023 Service Members of the Year

Psychedelics, cryotherapy and new treatments for vets | Defense News Weekly Full Episode 11.18.23

As a veteran, what should I look for in a future employer? — Money Minute

How 'artsy-fartsy stuff' can help vets recuperate and cope after service



A painting of Thomas Jefferson, circa 1800, by Rembrandt Peale.

The Founding Fathers have done more for U.S. strategic cyber resiliency than other modern initiatives. Their contribution is a stable society, that can absorb attacks without falling into chaos, mayhem, and entropy. Stable countries have a significant advantage in future nation-state cyber-information conflicts. If nation states seek to conduct decisive cyberwar, victory will not come from anecdotal exploits, but instead by launching systematic, destabilizing attacks on the targeted society that bring them down to the point that they are subject to foreign will. Societal stability is not created overnight, it is the product of decades and even centuries of good government, civil liberties, fairness, and trust building.

Why does it matter? Because the strategic tools to bring down and degrade a society will not provide the effects sought. That means for an adversary seeking strategic advantages by attacking U.S. critical infrastructure the risk of retribution can outweigh the benefit.

Ad

Ad

Ad

The black out in the northeast in 2003 is an example of how an American population will react when a significant share of critical infrastructure is degraded by hostile cyberattacks. The reaction showed that instead of imploding into chaos and looting, the affected population acted orderly and helped strangers. They demonstrated a high degree of resiliency. The reason why Americans act orderly and have such resiliency is a product of how we have designed our society, which leads back to the Founding Fathers. Americans are invested in the success of their society. Therefore, they do not turn on each other in a crisis.

Historically, the tactic of attacking a stable society by generating hardship has failed more than it has succeeded. One example is the Blitz 1940, the German bombings of metropolitan areas and infrastructure, which only hardened the British resistance against Nazi-Germany. After Dunkirk, several British parliamentarians were in favor of a separate peace with Germany. After the blitz, British politicians were united against Germany and fought Nazi Germany single-handed until USSR and United States entered the war.

The cornerstone for any society is institutions. The institutional resilience varies by nation, from stable democracies to totalitarian states on the brink of chaos and entropy. If we now flip this and look at potential adversaries, not one potential adversary is a stable society. These countries are totalitarian, authoritarian, and there is no

transition of power through elections or channels to canalize the will of the people. Several of these states have more to fear from the wrath of their own people than potential enemies. Authority is maintained using force, suppression, and manipulation. I met once retired Air Force Gen. John Shaud, who made a remark that the People's Liberation Army is "one-third army and two-thirds crowd control." The peace and daily order in China are products of suppression and totalitarian rule. In other words, if these authoritarian powers are removed, the society can quickly disintegrate. Any potential adversary takes a significant risk by using cyberattacks against the United States' critical infrastructure at scale. Why? Because the attacker is more dependent on stability for regime survival than the potential effects that can be reached in attacking the United States.

Ad

A strategic cyber campaign will fail to destabilize the targeted society if the institutions remain intact following the assault or successfully operate in a degraded environment. From an American perspective, it is crucial for a defender to ensure the cyberattacks never reach the magnitude that forces society over the threshold to entropy. In America's favor, the threshold is far higher than our potential adversaries'. By guarding what we believe in –

Trending Now

1. Pentagon approves first Rapid Defense Experimentation Reserve projects
2. Backpack jammer prototyped by CACI's Mastodon passes early Army test
3. Pentagon's commercial tech arm to ramp up role in military innovation
4. US, Australia eye joint hypersonics experiments in 2024
5. USS Carney responds to multiple attacks on commercial ships in Red Sea

fairness, opportunity, liberty, equality, and an open and free democracy – America can become more resilient.

We generally underestimate how stable America is, especially compared to potential foreign adversaries. There is a deterrent embedded in that fact: the risks for an adversary might outweigh the potential gains.

Jan Kallberg is a research scientist at the Army Cyber Institute at West Point and an assistant professor in the department of social sciences at the United States Military Academy. The views expressed are those of the author and do not reflect the official policy or position of the Army Cyber Institute at West Point, the United States Military Academy or the Department of Defense.

Share:

Ad