OODA LOOP

20 Red Teaming Lessons Learned

Matt Devost
OODA LLC
@mattdevost

Matt Devost

is a technologist, entrepreneur, and international security expert specializing in cybersecurity, counterterrorism, critical infrastructure protection, intelligence, and risk management issues.

TOTAL INTELLIGENCE SOLUTIONS
THE EVOLUTION OF INTELLIGENCE
TERRORISM RESEARCH CENTER
OODA
SAIC
From Science to Solutions
Security Design INTERNATIONAL
FUSIONX
iSIGHTPARTNERS
iDEFENSE
THE POWER OF INTELLIGENCE
accenture

We’ve been discussing these issues for over 20 years and it is a matter of be careful what you ask for.

We have fully arrived.

“The future has already arrived it’s just not evenly distributed yet.”

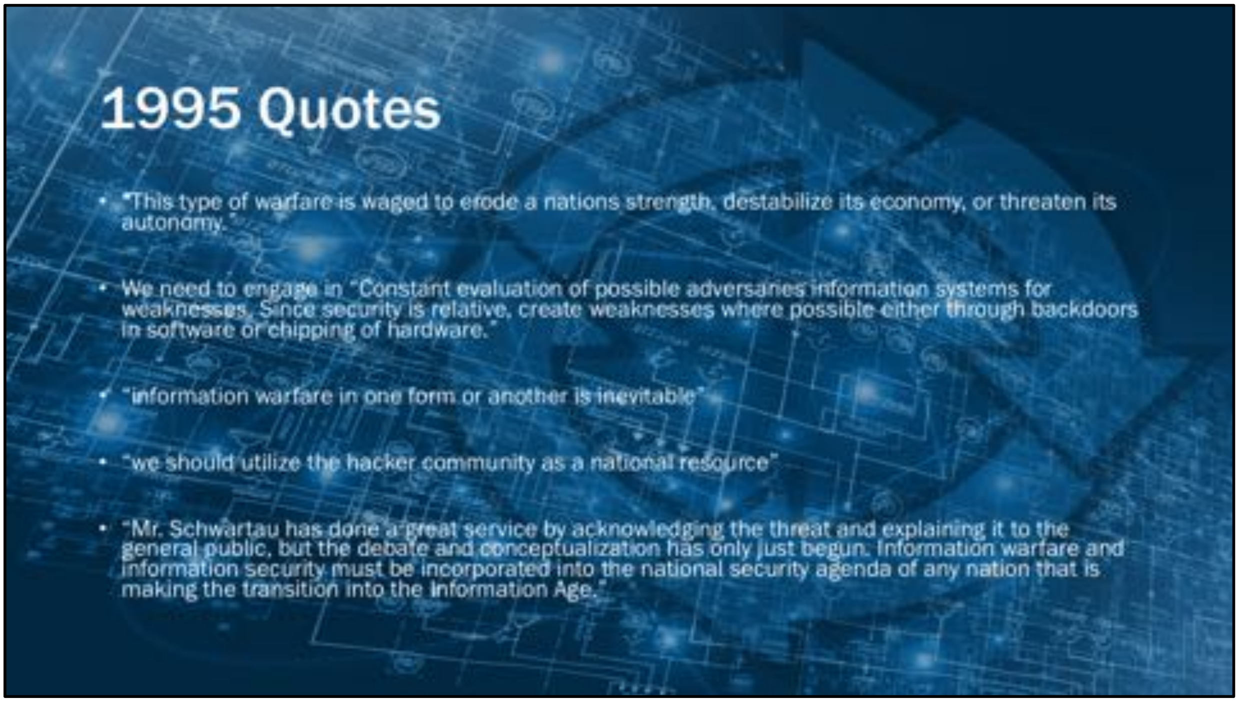
William Gibson

InfoWarCon is where the future arrives first.

“Information warfare is undoubtedly the warfare of the future.” - 1995

Political Aspects of Class III Information Warfare: Global Conflict and Terrorism.

In FUCKING January in Montreal



1995 Quotes

- "This type of warfare is waged to erode a nations strength, destabilize its economy, or threaten its autonomy."
- We need to engage in "Constant evaluation of possible adversaries information systems for weaknesses. Since security is relative, create weaknesses where possible either through backdoors in software or chipping of hardware."
- "information warfare in one form or another is inevitable"
- "we should utilize the hacker community as a national resource"
- "Mr. Schwartau has done a great service by acknowledging the threat and explaining it to the general public, but the debate and conceptualization has only just begun. Information warfare and information security must be incorporated into the national security agenda of any nation that is making the transition into the Information Age."

CAN YOU TRUST YOUR TOASTER?

Image source: Atlantic Magazine

Can You Trust Your Toaster – collaboration a result of InfoWarCon introduction by Betty O’hearn.

Never Fly Again (not well received)

2001 - Attackers will start “hacking belief systems”.

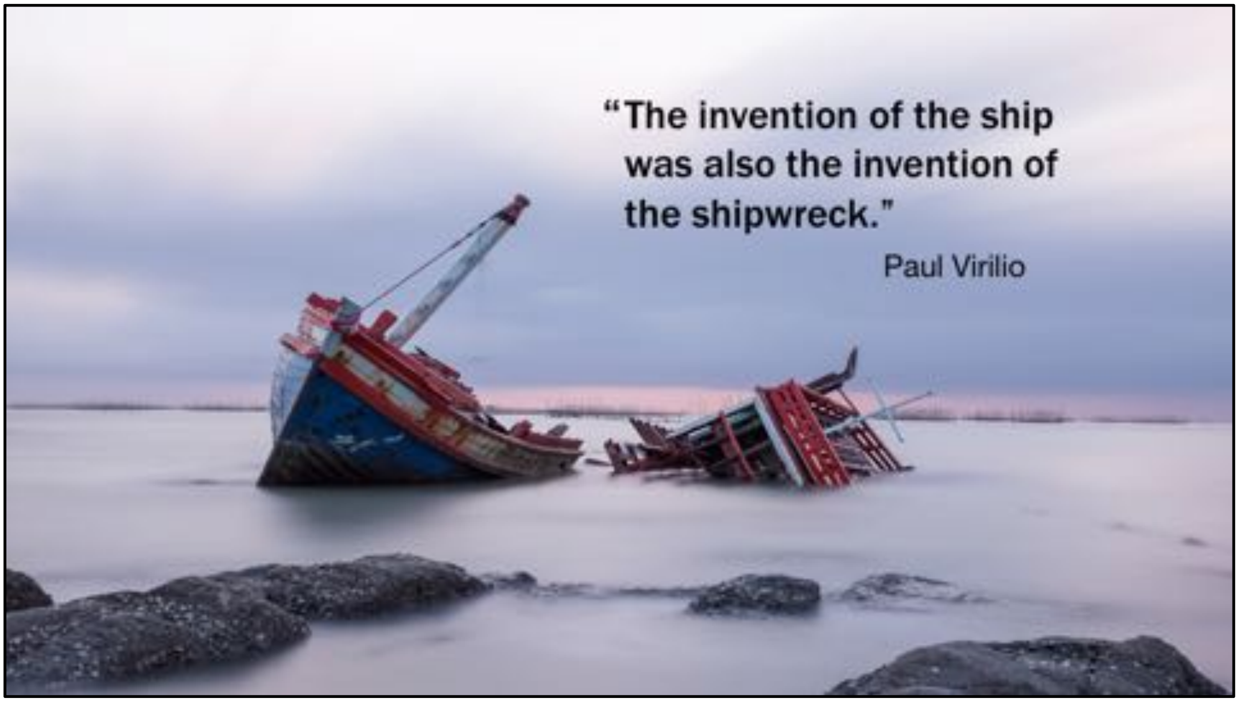
What I said at InfoWarCon 2001

“We have not yet realized our

FUTURE SHOCK potential.”

2015

What I said at infoWarCon 2015

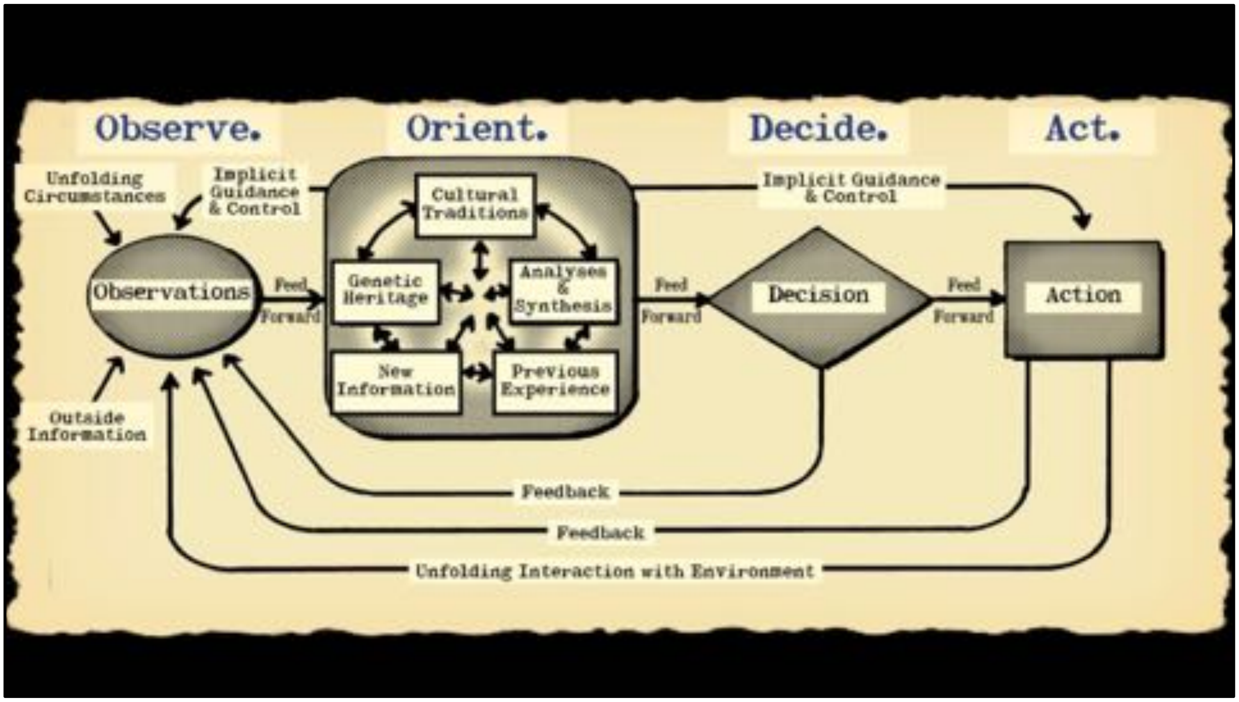


“The invention of the ship was also the invention of the shipwreck.”

Paul Virilio

Great analogy for where we are with internet. Great benefit with inherent vulnerability.

The adage that the Jedi want to bring balance to the force is a farce. Adversaries, competitors, and other actors/entities never seek balance. They seek asymmetry. Over time, I've come to recognize that order does not equate with balance, and the scales are never equally weighted regardless of whether we are talking international relations, economics, or societal frameworks like civil liberties versus security. Asymmetry is a key objective of the red teamer. This point was highlighted for me with Michael Moore's presentation at the Boyd & Beyond conference when he advocated that the concept of Yin and Yang is a lie. We always seek advantage, or at least less disadvantage, and that needs to be the guiding ethos of your red team. Out smart, out play, and be driven to actually win something. You can drive asymmetry through overwhelming force, technology or tactical surprise, attacks of disproportionality, or long-term strategy.



We have to assume that in an age of machine enabled information operations we might have a compressed OODA Loop

No Artificial Constraints

Yu can’t impose any constraints on the red team that you can’t also impose on the adversary.

Mention Van Riper story.

Someone once asked me what is FusionX’s red team methodology.

There is no spoon.

Can’t have a methodology.

A methodology is an artificial constraint on the red team. To truly red team, you need to unleash the creativity and ingenuity of the experts on the team. The key is not to think outside the box, but to think without the box.

Context is King

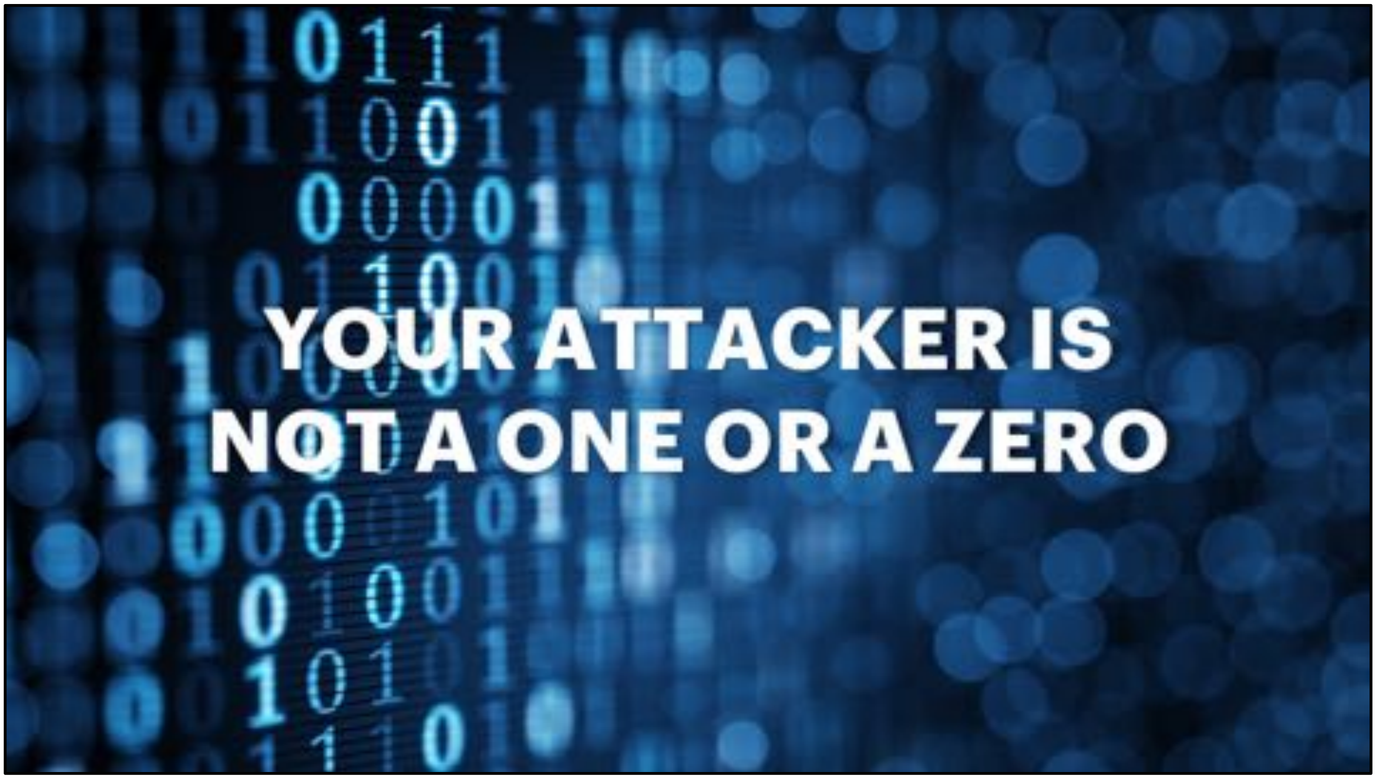
A successful red team can articulate their results in a way that brings context to the red team’s sponsor and supports their decision making process. Your red team briefing should have a valid threat/competitor model, an attack narrative with contextual outcomes, and the value proposition for the attacker and the defender.

Why we changed our red team reporting scale to articulate the real risk the business/organization.

Robert Garigue

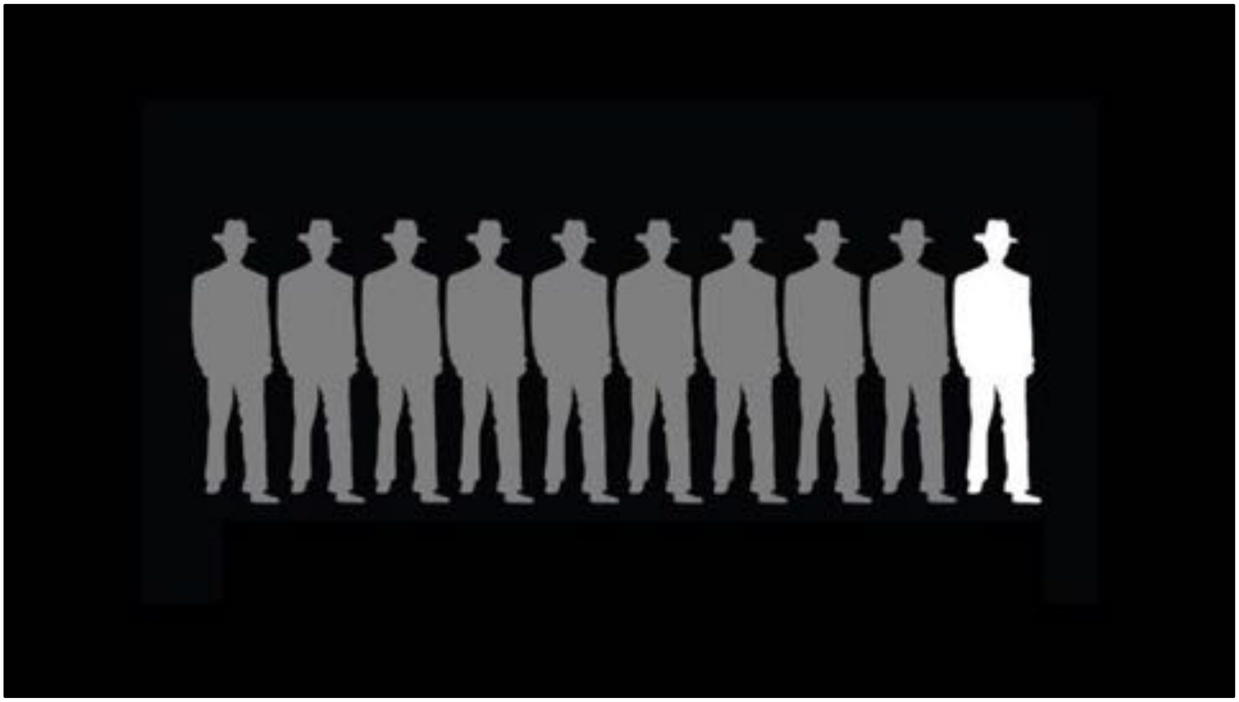
Tools are an essential enabler for a red team, but they do not make the red team. If you want a tool-driven red team, focus your R&D staff on creating tools based upon red team requirements, not vice versa.

When an IT security organization tells us that they red team by running Nessus or Metasploit, we'd often ask "what nation state does Nessus represent?" Tools are intent agnostic. An adversary is not. Tools treat all systems as equal. An adversary does not. There is great value in pro-actively probing your network with available tools, but they are not a replacement for a real human-led red team. By that same manner, there is great value to exercises conducted with structured injects, but a real red team takes place in real-time and is unscripted.



YOUR ATTACKER IS NOT A ONE OR A ZERO

Jason Healey first articulated this concept years ago to focus our attention away from the noise on the wire and back on the living, breathing, human adversary on the other side. You can't think of your adversary only in the context of the technical attack that manifests itself, but rather in the context of their human behavior. A good red team will re-enforce this fact for the blue team.



As humans we are fundamentally flawed towards consensus, hive mind, and an inherent desire to believe the lie. A good red teamer has to break outside the chains of conception and imagine the unimaginable and see whether the unimaginable can manifest itself as red action. Here the 10th man rule has great value, not in requiring the 10th man to automatically dissent, but also as a mental exercise to expand the potential of the red team. As a red teamer your job is to help prevent failures of imagination.

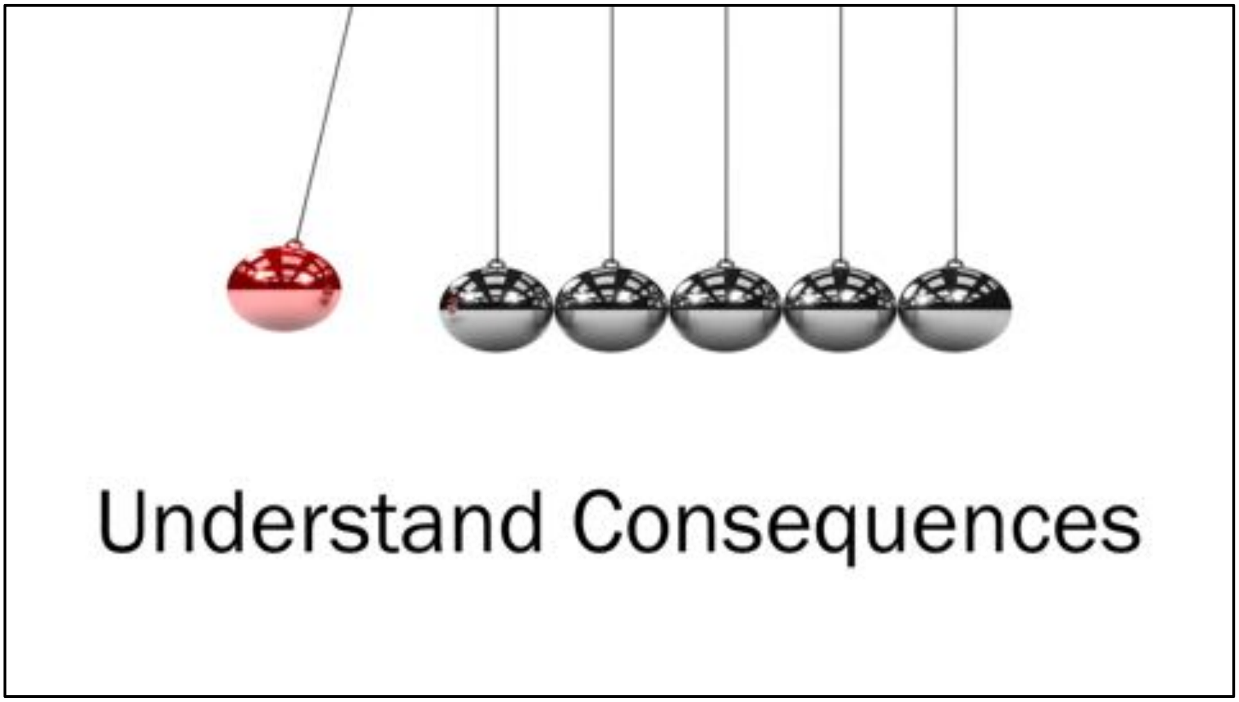
A red team should never compromise the integrity of their results to satisfy the red team sponsor. True value comes from speaking truth to power which often means articulating unpopular findings or diverging from the status quo or common conceptions.

One character password SOCOM story.

Don’t call it luck

Where you are is a result of work you put it, training, decisions you made.

If you attribute it to luck, you are doing yourself a disservice.



Understand Consequences

Downstream effects.

Impact to the business or organizational mission.

STRATEGIC PENETRATION FOR FUTURE EXPLOITATION

Think in terms of multiple adversarial pathways

Chinese might see a path of prosperity and also a pathway of conflict.

They are obligated to plan for both.

World War II ball bearing plant example.

Think in terms of time shifted intent.

Adversary doesn’t have current intent, but might they have future intent?

EVERY CYBER ATTACKER
IS AN INSIDER

Eventually, every attacker is an insider. Only a matter of time and resources.

How does your security model change if you presume breach?

You can’t spell security without IT

We have to acknowledge the fundamental role IT and hygiene play in cyber security.

Story of CEO who wanted to install network IDS.

NTSB for Cyber Attacks

We do a bad job of learning from attacks. Getting better, but still not good.

Read the book Black Box Thinking

Security in the Design Process

Must build security into the design process.

Dr. Lukasik (Director of ARPA at formation of ARPAnet) said that had they known it was important they would have thought about security.

We know IOT and other things are important now, but we aren’t building security in. Fundamental failing of industry right now.

Story about red team against IP satellite company.

Need to teach our blue teams to see the gorilla.

Read the Invisible Gorilla book.

Can’t be just eyes on glass. Need to active hunt.

Need to teach defenders to think like attackers.

No silver bullets

“NO PLAN SURVIVES CONTACT WITH THE ENEMY.”

MILITARY STRATEGIST HELMUTH VON MOLTKE

Eisenhower said ”Plans are worthless, but planning is everything”

Eric Haines : “Some people say planning is everything and for those that never execute, maybe it is.”

Build adaptive and resilient teams.

A red team is like a sparring partner.

Would you train to fight Mike Tyson with a static punching bag or a sparring partner?

Targeting Trust

Trust is a target.

We failed to predict how critical this would be 20 years ago.

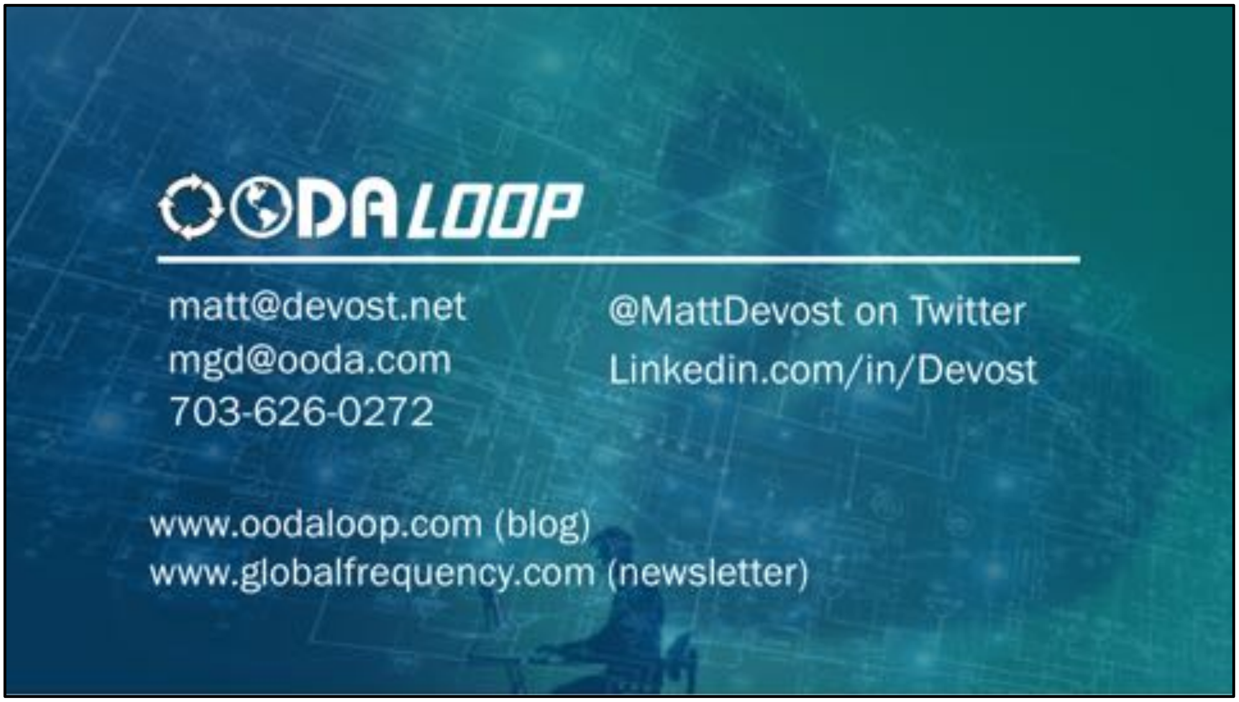
Must maintain trust in organizations (banks, etc).

Must maintain trust in institutions and processes (voting, etc).

Must think about trust as a target in our threat models.

OODA.CO/redteamlessons

Read the original 10 lessons learned here.



OODA LOOP

matt@devost.net
mgd@ooda.com
703-626-0272

@MattDevost on Twitter
Linkedin.com/in/Devost

www.oodaloop.com (blog)
www.globalfrequency.com (newsletter)

OODALoop.com is where I publish a lot of my thinking on these issues.

Global Frequency is my weekly mailing list highlighting top stories of the week and one book recommendation.

Connect with me on social media and Twitter.