

Cyberwar is Bullshit

Marcus J. Ranum

CSO, Tenable Network Security

Crime, Terror, War

- 3 *very* different things; do not let people confuse you about that!

Cybercriminal

- Agenda:
 - Diffuse and profit-driven
 - Non-strategic: short-term
- The threat:
 - Hit and run
 - Cannot eradicate: more will take their place
 - Creative
 - Rapidly shift to where the money is

Cyberterrorist

- Agenda:
 - Ideological maximum-damage highly public attacks with no restraint
 - **Fear** not just costly damage
- The threat:
 - Targets will be civilian infrastructure that results in explosions, destruction and death
 - Power, water, oil, shipping, vehicle control

The cyberterror paradox

- There is huge room for potential growth in cyberterror
 - Why hasn't it happened yet?
- There is ***gigantic*** room for cyberterror attacks aimed at economic damage
 - Why hasn't it happened yet?

The cyberterror paradox: 2

- The most technologically sophisticated nations are the ones that are easiest / most likely to be successfully attacked by cyberterrorists
 - They are also the ones most likely to successfully weather such attacks
 - ...and are the easiest to hurt with low-tech high impact attacks like 9/11

Cyber Spy

- Agenda:
 - Surreptitiously gather secrets from a target
 - Suborn and manage trusted agents in critical positions
- The threat:
 - The cyber-era simplifies some technical aspects of espionage a bit while complicating others a bit

Cyberwarrior

- Agenda:
 - Be prepared to attack/degrade/penetrate enemy command and control systems as an adjunct to physical military operations
- The threat:
 - ?

Battlefield of the Future?

- There are (at least) 5 huge buried paradoxes in the notion of cyberwar
 - The disarmament effect
 - The cost factor
 - Packets don't hold ground
 - The “Blind Mike Tyson Effect”
 - The “who'd win anyhow” question

Visualize whirled peas

- The disarmament effect
 - Imagine what happens if you're the commandant of the cyber-strike force
- ...and D-day is patch Tuesday?

The cost factor

- To attack a network, you have to have effective management control over it (unless you're just DOSsing it, in which case your attack may be deflectable)
 - Therefore: cyberwar == involuntary remote system administration
 - So, we need, what, **a combat version of UniCenter?** See where this is going?

Packets don't hold ground

- Before an attack is launched it needs to fulfil some useful military objective (to take or hold ground or destroy physical materials)
 - Taking and holding ground implies tactical and strategic superiority for the follow-through
 - Therefore cyberwar only makes sense *to the side that is likely to win anyhow*

The “blind Mike Tyson Effect”

- Many proponents of cyberwar propose it could be used to temporarily degrade an enemy’s command/control or intelligence for tactical advantage
 - Blinding a superpower, even temporarily, invites a massive fear-triggered response
 - “Blind me, I nuke you.”
 - This option only makes sense *to the side that is likely to win anyhow*

The “who’d win anyhow” question

- Cyberwar is almost entirely only useful in two situations:
 - 1) a scorched-earth defense, in which the defender just wants to inflict damage as they die
 - 2) by the *side that is likely to win anyhow*
- This means the US is the most likely to use cyberwar

The Future

- Cyberwar doesn't have much of a future, in the short term (next decade or two) until there are more highly technological mutually hostile superpowers
 - It's pointless for a superpower to develop cyberwar techniques to attack a non-superpower (they can just crush them conventionally)

When is cyberwar “state-sponsored cyberterror”?

- When the targets are civilian infrastructure!
 - A country’s automatic teller network is not a military target
 - A country’s financial exchange system is not a military target!
- I am *deeply* concerned that our political leaders will bring *total warfare* into cyberspace; I.e.: **cyberwarcrime**

Broad Predictions

- Cybercrime: huge problem; will grow vastly worse
- Cyberterror: not a problem yet; potential to grow horrible is not being realized
- Cyberespionage: business as usual; will continue as usual
- Cyberwarfare: largely vapor; will remain largely vapor

Summary

- No matter how you slice it, critical civilian infrastructure will come under increasing cyber-attack
 - But cyber*war* is bullshit