# Cyberwar in the age of Total War

**Marcus J. Ranum**
<mjr@tenable.com>
CSO, Tenable Network Security, Inc.

## Who Am I?

- Industry insider for the last 25 years
  - Early innovator in firewall, VPN, and IDS technology
  - Started as a software engineer
  - Have held every position possible in high-tech start-ups from system administrator to marketing, sales, presales, director of engineering, CTO, CSO, CEO
  - Currently CSO of Tenable

## Why This Talk?

- Cyberwar is now becoming an important part of the cyber-security industrial complex
  - At least, financially
- We don't want to be like the atom bomb builders, standing around years later asking "what did we do wrong?" Do we?

## Hard

- The difficulty with writing this talk:
  - Attempt #1: historical perspective, including a sober rationale for the evolution of rules of warfare since the Treaty of Westphalia
  - Attempt #2: philosophical arguments, based on moral reasoning with a semi-utilitarian perspective
  - Attempt #3: I just want to scream

## Historical Perspective

- The problem with approaching cyberwar historically is that every attempt in history to oppose militarization has failed
  - Consistently violated by the powerful whenever it's to their advantage
  - Regulation, in fact, is in service of the powerful (e.g.: nuclear non-proliferation)

## Philosophical Arguments

- Approaching war philosophically becomes an exercise in the obvious:
  - It's immoral
  - Involving civilians ought to be avoided
  - etc.
- These are statements of the obvious, and the fact that they're consistently ignored is equally obvious

## Screaming

- A message is not heard if it's delivered unpleasantly

## In Case You Were Sleeping

- Modern states based on principles established in Treaty of Westphalia:*
  - In return for monopoly on violence there's a bright line between acts of state and its agents and those of the citizen
  - Citizens can't declare war on a state, nor a state on a citizen
  - *No more* issuing letters of marque and reprisal (authorizing an individual to make war on a state as a free agent)

* 1648

## Sovereignty

- Under Westphalian notion of state, states are in control within their borders
  - Have negotiated (part of international law) relationships for trade and what happens when their citizens visit/do business within other states
  - In principle, states don't interfere with each other (ha!)

## Sovereignty

- Obvious challenges to sovereignty are:
  - Wars of aggression
  - Internal collapse (e.x: Somalia) - permanent civil war - so called "failed states"
    - Humanitarian intervention may be justified

## Sovereignty

- Terrorism allegedly presents a problem in this context:
  - If a nation is responsible for its acts and is responsible for policing its people
    - What about states that harbor terrorists?
    - What about terrorists that are not actually harbored by the state?

## Terrorism and International Law

- There is no agreed upon definition of "terrorism" in international law
  - At one of the spectrum are the anarchists who say 'all actions of the state are terroristic'
  - At the other end of the spectrum are the conservatives who say 'states *can't* do terrorism' because it's illegal and states define laws*

* basically, begging the question

## Some Things We Know:

- The prior concern of international law with respect to “declarations of war” existed *for this reason*!
  - In time of war it’s “a commando raid” not an act of state-sponsored terrorism
  - In the framework of declared wars, things are pretty cut and dried
- Let’s look at “states of war”

## The Era of 4GW

- 4th Generation Warfare (aka: “little wars” “low-intensity conflict” or “endless war”)
  - Today’s norm
  - When was the last “declared war”?
  - This is a *moot point* (see next)

## Enter the Geneva Convention

"In addition to the provisions which shall be implemented in peace time, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."*

*Convention IV 1949

## Geneva Convention *(cont)*

- Article III covers non-international conflicts
  - "The principle of respect for human personality, the basis on which all the Conventions rest, had found expression in them only in its application to military personnel. Actually, however, it was concerned with people as human beings, without regard to their uniform, their allegiance, their race or their beliefs, without regard even to any obligations which the authority on which they depended might have assumed in their name or in their behalf."*

*ICRC commentary on Convention III 1929

## In Other Words...

- The line between “state-sponsored terrorism” and “armed conflict” is a bit brighter and clearer
  - A philosopher might argue that the issue is *attribution* - an “armed conflict” involves the notion that ***you know who’s attacking*** you, whereas “state-sponsored terrorism” attempts to destabilize the target without attribution of the attack

## State-Sponsored Terror

- Thus we argue that “state-sponsored terror” is when a state adopts the technique of terror rather than armed conflict
  - Corollary: a terrorist operating within a state that repudiates their actions will either be thought to be a “terrorist” or “state-sponsored” to the degree to which they can be attributed as an agent of the state

## The Elusive "Terrorism"

- Terrorism is either:
  - A crime
  - A violation of the laws of war
- I don't want to try to resolve this one because it's actually not relevant
  - Because *either way* the international community has mechanisms for dealing with it

## Divertimento: Espionage

- Much ado is made regarding state-sponsored espionage via cyberspace
  - Sometimes this is referred to as a "cyberattack"
  - Again:
    - covered either under international humanitarian law*
    - or treated as a crime if not during an armed conflict

* Protocol 1, part III article 46 Geneva Conventions of 1949, June 1977

# On to “Cyberwar”

- Never mind the word “war” behind the word “cyber-”
  - The questions to examine are:
    - Are the laws of war (Geneva Convention and Protocols) being followed?
    - Is it attributed?

# Case Study: Bushehr

- Stuxnet

  “Art 56. Protection of works and installations containing dangerous forces

  1. Works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population.”
- The control systems attacked were coolant pumps

* Protocol 1, addition to Geneva Conventions of 1949, June 1977

## Stuxnet

- Was Stuxnet:
  - State-sponsored terrorism
  - A violation of international humanitarian law
  - Both

## Reprisal

- During conflict (not necessarily a declared state of war) under the GC a limited deliberate violation of the laws of war may be taken in *reprisal*
  - Not to be confused with *retorsions* which are legal retaliations like punitive tariffs
  - Generally reprisals are limited by *proportionality* because of the danger of involving civilians

## Reprisal for Stuxnet?

- Would Iran be justified in launching a cyber attack against the US or Israel in response to Stuxnet?
  - This is a serious question
  - Especially if the answer is “yes”
- Let’s dismiss that as a hypothetical, though

## Stuxnet a War Crime?

- It was either:
  - State-sponsored terrorism
  - War crime
- There is ***no*** 3rd alternative
  - Arguing it was state-sponsored terrorism (I.e: outside of an armed conflict) is “better” because it removes justification for reprisal

## Oops I Was Wrong:

- There is an “option 3” - if some government were hosting whoever ordered the release of Stuxnet, declare them “unlawful combatants” and hand then over to Iran

## Cyberwar in Libya

- “In the days before President Obama approved American-led airstrikes in Libya without congressional go-ahead, the White House considered using cyberwarfare”

## Here's the Problem

- Cyberwar cannot, will not, ever be fought over military networks
  - Components of civilian infrastructure will carry the data
  - Components of civilian infrastructure will be some of the targets

## Again: International Law

- "The parties to the conflict must at all times distinguish between civilian objects and military objectives. Attacks may only be directed against military objectives. Attacks must not be directed against civilian objects."*

* Rule 7
Customary International Humanitarian Law, ICRC

# Proportionality

- Many like to point out:

  "Launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited."*

- That's not a hunting license!
  - Go read Rule(s) 13 and 15 if you're curious
  - The doctrine of proportionality is intended to be an individual's *argument of defense* if they wind up on trial for war crimes

* Rule 14
Customary International Humanitarian Law, ICRC

# The Dangerous and Likely Outcome

- My fear* is that "cyberwar" will become a plaything of the powerful
  - *We* will use it on *you* but don't you ***dare*** use it on us

"If you shoot me in a dream, you'd better wake up and apologize"
- Mr. White, "Reservoir Dogs"

* prediction, actually

## Why It's Dangerous

- Use of main force is great when you're the top dog
  - … But you know that eventually you will find yourself unable to retaliate, and without a shred of moral high ground to complain from

## Conclusions

- We are at a crucial time in the militarization of cyberspace
  - What example will security practitioners set?
  - Engaging purely in defensive operations is the only position without moral onus

"If you shut down our power grid, maybe we will put a missile down one of your smokestacks."

- Pentagon Spokesman

Rule 151. Individuals are criminally responsible for war crimes they commit.*

* Customary International Humanitarian Law, ICRC

# Farewell

- I beg ISSA to undertake ***establishing an official position prohibiting involvement of its professional members in war crimes or state-sponsored terror in cyberspace***