THE UNITED STATES
CYBER CONSEQUENCES UNIT

How Cyber Attacks Will Be Used in International Conflicts

Scott Borg

Director and Chief Economist

US Cyber Consequences Unit

www.usccu.us

All cyber security efforts today could potentially become embroiled in military conflicts between nation states!

Why would a nation state bother with cyber attacks?

REASONS CYBER-ATTACKS WOULD BE A TEMPTING MILITARY OPTION FOR NATION STATES – PART I

1) They could selectively stop certain activities of a country or population, while leaving other activities unaffected

2) They could be carried out with less loss of life than any other attacks that cause comparable levels of destruction

3) They could allow many gradations of destruction across an extremely broad range of targets

4) They could be effective against some targets that are too well protected or too widely dispersed to be reached otherwise

REASONS CYBER-ATTACKS WOULD BE A TEMPTING MILITARY OPTION FOR NATION STATES – PART II

5) They could target the central components of contemporary military technology in a uniquely direct way

6) They could be effectively combined with almost any other kind of military operation

7) They could allow nation states to exploit kinds of anonymity and ambiguity that are ordinarily only available to small, non-governmental organizations

8) Their effects could sometimes be partially reversible at the discretion of the attacker

Possible Cyber-Attack Allies for National Governments:

- Ideological Militants
- Ethno-Nationalists
- Criminal Enterprises
- Vindictive Insiders

→ Major Opportunities for Governments to Employ Cyber Attacks Indirectly!

SOME NOTABLE CYBER CONFLICTS - I

1998 – Zapatista sympathizers (inc. Italians, Austrians, & Dutch) vs. Mexico (also U.S. DoD & Frankfurt Stock Exchange)

1998 – Pakistan vs. India (after nuclear tests)

1999 – NATO (in Kosovo) vs. Serbians (and Russians)

1999 – China vs. U.S. (after Chinese Embassy in Belgrade bombed)

1999 – China vs. Taiwan

1999 – India vs. Pakistan (during armed conflict in Kashmir)

1999- – Hamas vs. Israel

2000- – Azerbaijan and Turkey vs. Armenia

2000- – Hezbollah vs. Israel

2001 – China vs. U.S. (after U.S. spy plane collision)

2002- – Animal rights activists, white supremacists, etc.

2005 – Indonesia vs. Malaysia (dispute over control of Celebes Sea)

SOME NOTEABLE CYBER CONFLICTS - II

2005 – China & South Korea vs. Japan (dispute over Japan's refusal to acknowledge war crimes)

2005 – German Neo-Nazis vs. the world

2006 – Muslims vs. Denmark (after Mohammed cartoon)

2007 – Russia vs. Estonia

2007 – Israel vs. Syria (supporting air attack)

2008 – Russia vs. Lithuania (300 websites defaced)

2008 – Russia vs. Georgia

2009 – Russia vs. Kyrgystan (two of four ISP's shut down)

2009 – Russia vs. Kazakhstan (news agencies)

2009 – North Korea (?) vs. South Korea & U.S.

- Cyber attacks now a standard accompaniment of nearly all serious conflicts
- Government wishes carried out without need for any overt government actions
- Cooperation from organized crime
- Social networking as an organizational tool
- Highly controlled societies like Russia and China have an advantage
- Complementing military actions in specific ways
- Potential for doing physical damage to critical infrastructure industries
- Individual companies and organizations threatened
- Economic motives

A KEY CONSEQUENCE: REGIONAL CONFLICTS COULD DISRUPT GLOBAL SUPPLY CHAINS

Example 1: Business Process Outsourcing to India

BPO's are characterized by "function creep": they leverage their inside knowledge of their clients' businesses to expand services at an *irresistibly*
low cost

- Initial services provided: back office accounting, transaction processing, programming, customer call centers
- Further services provided: customer relationship management, IT design and development
- Future services beginning to be provided: actuarial services, credit analysis, risk management, regulatory compliance, asset valuation

(Example 1: Business Process Outsourcing to India, continued)

- BPO's would be *most* hurt by attacks that would cause them to produce defective information and services, discrediting them as companies
- Defective information from BPO's could create uncertainty about asset valuations and the relative risks of investments
- This, in turn, could cause a stampede of capital away from the institutions where BPO-produced valuations were put in doubt

Example 2: Electronic Components Produced in Southeast Asia

- Production is often concentrated in three or four neighboring countries
- American inventories are often limited and deliveries are often on a just-in-time basis
- Although often treated as a commodity, tailoring the output to a particular manufacturer-customer takes a minimum of several weeks

What about when governments employ cyber attacks *directly*?

— Either in conjunction with physical attacks, or as pure cyber attacks?

When should the commander of a physical attack consider adding cyber attacks?

THE SIX WAYS CYBER ATTACKS COULD CONTRIBUTE TO PHYSICAL ATTACKS (Borg Analysis) - PART I	
1) Critical Targeting Information	determining the target's physical location determining the target's defensive capabilities determining the target's physical vulnerabilities
2) Physical Access to the Target	providing passage through security barriers drawing the targets into vulnerable positions

THE SIX WAYS CYBER ATTACKS COULD CONTRIBUTE TO PHYSICAL ATTACKS - PART II	
3) Cover for the Attacking Force	blinding the adversary to what is happening or where confusing the adversary with false information causing diversions that would absorb the adversary's attention
4) Interference with Counter-Attacks	interrupting activities needed to launch counter-attacks damaging equipment needed to launch counter-attacks

THE SIX WAYS CYBER ATTACKS COULD CONTRIBUTE TO PHYSICAL ATTACKS - PART III	
5) Magnification of Consequences	encouraging activities before the attack that will increase losses interfering with efforts after the attack to limit losses damaging systems that could substitute for those attacked
6) Parallel Attacks on the Same Targets	hitting targets that the physical attack might miss damaging aspects of targets unharmed by the physical attack

How much damage could cyber attacks do *alone*?

Critical Infrastructure Industry	Direct Percent of GDP	Effective Percent of GDP	Dependent Percent of GDP
Electric Power	1.5	3.4	72
Oil and Gas Fuel	1.0	3.0	71
Telecom & Internet	2.6	4.9	62
Banking and Finance	5.7	8.6	59
Water and Sanitation	< 1	< 1	40
Chemical Industries	1.7	4.1	33
Air Transport	0.5	2.0	24
Ground Transport	2.1	4.0	(62)
Hospitals and Health Care	6.7	15.4	16

Special Features of Cyber Attacks on Critical Infrastructure Industries

- Generally prepared long in advance by inserting malware into the target systems
- Deployed with multiple types of cyber attacks on each target
- The triggering signal or mechanism is usually the trickiest component
- Subject to spoofing of damages

Why can't we employ deterrence?

REASONS WHY DETERRENCE IS NOT AN EFFECTIVE POLICY FOR DEALING WITH CYBER-ATTACKS - PART I

1) Uncertainty about who is responsible for any given cyber attack, their motives, and their longer term agenda

2) Degrees and types of responsibility that are difficult to classify, even when the facts are known

3) No assurance that a retaliatory cyber attack will succeed

4) Considerable danger that a retaliatory cyber attack will have unintended consequences

REASONS WHY DETERRENCE IS NOT AN EFFECTIVE POLICY FOR DEALING WITH CYBER-ATTACKS - PART II

5) No way to be sure exactly what damage has been done by a retaliatory cyber attack after it has been carried out

6) No credible formula for an appropriate physical response to an attack that is purely cyber

7) No reason to believe that dispersed, civilian would be deterred by a potential counter-attack on any reachable target

8) High cost of retaliation if the target is the collection of individuals responsible for the initial cyber attack

Where does this leave our overall defense strategy?

Different Adversaries, Different Goals

CYBER-DEFENSE REVOLUTION IN MILITARY AFFAIRS (Borg Synthesis) - 1		
	Industrial Defense Era	**Cyber-Defense Era**
Central Principles	Nation states as adversaries	Networked groups as adversaries
	Concentrated forces	Diffuse forces
	Fire power advantage	Information advantage
	Aspiring to intimidating force	Aspiring to ubiquitous force

No More Incomings, No More Invading Forces

CYBER-DEFENSE REVOLUTION IN MILITARY AFFAIRS - 2		
	Industrial Defense Era	**Cyber-Defense Era**
Strategy	Defending perimeters of geographical areas from attacks originating outside	Defending internal networks and operations from attacks appearing inside
	Military and military-industrial targets	Critical infrastructure targets
	Success measured by destruction of equipment and infliction of casualties	Success measured by the protection or destruction of value
	Battlefield theory as central	Economic theory as central
	Deterrence-based policies	Resilience-based policies

Cyber-Attacks Are *Not* Primarily a "Force Multiplier"

CYBER-DEFENSE REVOLUTION IN MILITARY AFFAIRS - 3		
	Industrial Defense Era	**Cyber-Defense Era**
Tactics	Engagements between groups of men and weapons	Engagements between integrated systems with extensive automated programs
	Information systems as support	Information systems as weapons
	Speed and range in executing attack operations as crucial	Speed and coverage in identifying the nature and location of the adversary's operations as crucial
	Area and facility targeting	System and process targeting
	Destruction of targets	Hijacking or corruption of targets
	Assured results	Probabilistic results

Network Centric Warfare Was on the Right Track, But Didn't go Far Enough

CYBER-DEFENSE REVOLUTION IN MILITARY AFFAIRS - 4		
	Industrial Defense Era	**Cyber-Defense Era**
Decision Processes	Centralized decision-making	Flexibly distributed decision-making
	Emphasis on large group discipline	Emphasis on small group initiative
	Clarity about identity of adversary	Uncertainty about identity of adversary
	Problems with deducing patterns from insufficient information	Problems with recognizing patterns amid excess information

Thank you!

For more information or permission to use this material, please contact:

Scott Borg
US Cyber Consequences Unit
P.O. Box 1390
Norwich, VT 05055
Scott.Borg@usccu.us
802 – 649 - 3849