RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CXO-F01

Strategic Cyber Actions and How They Could Affect Your Company

Scott Borg
Director (CEO) and Chief Economist
U.S. Cyber Consequences Unit

Strategic Cyber Actions (SCA's)

- The main type of strategic actions in a global information economy
- Can be utilized both in benign, legitimate ways and in malign, illegitimate ways
- Will increasingly need to be employed by America & its allies
- Often only understandable in terms of global politics
- Can potentially put any organization with a significant internet presence on the front line

The Context for Strategic Cyber Actions

With the new possibilities for high-bandwidth, networked interaction . . .

- Economic conflict is no longer confined to markets
- Military conflict is no longer confined to battlefields
- Political conflict is no longer confined to diplomacy and elections
- Economic, military, and political conflicts are no longer separate

The World of Strategic Cyber Actions Is Already Here!

China & Russia seem to understand this better that the U.S. & the EU!

- Chinese effort to acquire competitively important business information to feed economic development
- Chinese effort to secure global control of key supply chains for critical industries
- Russian effort to gain influence or control over Eastern European countries
- Russian effort to promote Western politicians who would undermine NATO & the EU

Not Just a Matter for Nation States!

- ‘Sharing economy’ effort to avoid the traditional regulations imposed on services & rentals
- Oil industry effort to delay actions that would reduce global warming
- U.S. gun lobby effort to stop any limitations on the sale or deployment of firearms
- Anti-abortion campaign efforts to shut down any organizations that provide help in ending pregnancies
- Animal liberation movement effort to disrupt testing & other uses of animals

What Are the Features of a Strategic Cyber Action?

- Employs large numbers of computers
- Continues for months or longer
- Bypasses or subverts normal business operations, markets, & political institutions
- Employs cyber attacks, but not limited to cyber attacks
- Operates on multiple fronts, often using proxy agents
- Changes the information environment
- Aims to produce broad and lasting political or economic consequences

Who Launches & Guides Strategic Cyber Actions?

- National Governments
- Agencies Supposedly Controlled by Governments
- Large Corporations
- Industry Advocacy Groups
- Political Advocacy Groups
- Extremist Cults & Cabals
- Ad Hoc Groups Inspired by Emotional Causes
- Any group that can shape or direct the activities of a large number of computer users over an extended period of time

Who Actually Carries Out Strategic Cyber Actions?

- Criminal Enterprises
- Ad Hoc Freelancers
- Ethno-Nationalist Cyber Militias
- Individual Ethno-Nationalists
- Ideological Militants
- Emotionally Motivated Enthusiasts
- Subsidiary Units or Agencies
- Public Relations & Lobbying Firms
- Other Consultants & Contractors

How Does the Organizer of a Strategic Cyber Action Motivate & Control the Agents? (Part I)

Providing Relatively Direct Incentives:

- Directly paying the agents for their activities
- Promising to offer the agents future business opportunities
- Offering immunity from prosecution for cyber crimes
- Arranging for the agents to gain competitively useful information
- Allowing agents to hide other activities in the strategic action

How Does the Organizer of a Strategic Cyber Action Motivate & Control the Agents? (Part II)

Making the Activity Emotionally Satisfying:

- Appealing to the agents' ethno-nationalist sentiments
- Overtly associating the strategic action with some cause the agents want to advance
- Inciting anger with false information and making the strategic action a way to express that anger
- Deceiving agents about the effects of their actions by a false flag or other direct deception

What Do People Actually Do in Strategic Cyber Actions?

Activities that can be used to create more value *or* to appropriate and destroy value!

I. Manage Broader Information Flows

II. Intervene in Business Operations

III. Determine Market Conditions

I. Managing Information Flows

1) Massive creation or acquisition of competitively important information

Bright Side: e.g., helping businesses to identify opportunities

Dark Side: e.g., stealing production technology to undercut the companies that developed it

2) Propagation of information encouraging favorable political or business conditions

Bright Side: e.g., helping companies to see the advantages of international collaboration

Dark Side: e.g., causing confusion about which scientific findings, technologies, and businesses models are valid

II. Intervening in Business Operations

3) Strategic subsidy and coordination of complementary organizations, industries, or governments

Bright Side: e.g., helping to make global supply chains more secure

Dark Side: e.g., gaining control of critical suppliers to limit rivals' access to them

4) Interventions in the functions of an individual business, industry, or government to provide a competitive advantage

Bright Side: e.g., helping companies to develop better processes relative to global competitors

Dark Side: e.g., damaging rivals to increase their costs

III. Determining Market Conditions

5) Use of cyber or economic incentives or sanctions to influence market mechanisms

Bright Side: e.g., pressure local governments to reduce corruption and honor contracts more reliably

Dark Side: e.g., coerce or bribe local regulators to discriminate against rivals

6) Use of cyber or economic incentive or sanctions to determine who can participate in markets

Bright Side: e.g., reducing trade barriers for customers or suppliers

Dark Side: e.g., using cyber attacks and local regulations to make market entry more expensive

Actions to Take Immediately

- Identify the Strategic Cyber Actions (SCA's) that could affect your organization
- Identify the news developments that could make you an immediate target for these SCA's
- Identify the actions that could make you less of a target or less vulnerable (especially, the actions *outside* of cyber security)
- Identify the actions to take if an attack resulting from an SCA is imminent or underway

For questions, permission to use this material, or information on master classes, please contact:

Scott Borg
Director (CEO) and Chief Economist
U.S. Cyber Consequences Unit
scott.borg@usccu.us