Defining Offensive Cyber Capabilities

Diplo Foundation

Researchers:
Dragan Mladenović, Ph.D.
Vladimir Radunović

May 2018
Social Environment

Conventional armed conflict of two belligerent sides
(Kende, 1971)

Cold war, internal and proxy wars

Net-centric, Hybrid, Unrestricted conflicts
(Warden, 1995; Cebrowski & Garstka, 1998; Virilio, 1986, 2000; Liang and Xiangsui 1999; Gerasimov, 2013)
(with cyber capabilities as an ideal tool)

The traditional division of the period of armed conflict and peace is no longer applied in the practice of conflict, but it is applied in the practice of International Law.

“The saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom.” (Isaac Asimov, 1988).
Multidisciplinarity: To assess social, political, military, security, technology, and international law context.

Interdisciplinarity: To determine unique understanding of the subject of research from different angles of observation.

Cyber security:
- ICT security
- Technologies
- Processes
- Policies
- Rules
- Organization
- Norms
- Standards
- People
- Other related things

*Adapted from van Solms & van Niekerk
### Offensive Cyber Capabilities

<table>
<thead>
<tr>
<th>Actors</th>
<th>States (Military, Security-Intelligence, Law Enforcement)</th>
<th>Non-states (Business, legal and illegal organizations and groups, Individuals)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations domain</td>
<td>National</td>
<td>International</td>
</tr>
<tr>
<td>Objectives</td>
<td>In the jurisdiction of the states</td>
<td>Overlapping jurisdiction (coincidence of interest; coordination; cooperation, and coercion)</td>
</tr>
<tr>
<td></td>
<td>Overlapping jurisdiction (coincidence of interest; coordination; cooperation, and coercion)</td>
<td>Out of jurisdiction of States</td>
</tr>
<tr>
<td>Effects</td>
<td>Power Projection (denial, degradation, disruption, or destruction)</td>
<td>Manipulation/Influence</td>
</tr>
<tr>
<td>Military operations</td>
<td>Offensive</td>
<td>Defensive</td>
</tr>
<tr>
<td>Method/Technique</td>
<td>By use of cyber weapons</td>
<td>By conducting specific activities/techniques</td>
</tr>
<tr>
<td>International legal character</td>
<td>Source of Law Regulated Unregulated</td>
<td>In relation to State acceptance Accepted Not accepted</td>
</tr>
<tr>
<td></td>
<td>In relation to legality Legally Gray Zone Illegally</td>
<td>In relation to legality Legally Gray Zone Illegally</td>
</tr>
</tbody>
</table>
## State Use of Offensive Cyber Capabilities

<table>
<thead>
<tr>
<th>Subjects</th>
<th>(State entities) authorization by the constitution</th>
<th>Armed forces</th>
<th>Legal</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Depts. and Agencies</td>
<td>Authorization by Law</td>
<td>Security-Intelligence agencies</td>
<td></td>
</tr>
<tr>
<td>Non-State entities</td>
<td>Other non-govt. groups</td>
<td>Law enforcement</td>
<td></td>
</tr>
<tr>
<td>Other „special&quot; forms of collaboration</td>
<td>Organized by the govt.</td>
<td>Private business</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In mutual collaboration with the govt.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Military–industrial complex</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Providers of „raw products&quot;, Tools and Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Proxies</td>
<td>Legal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Executors</td>
<td>Legal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Volunteers</td>
<td>Legal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Territorial – civil forces</td>
<td>Legal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hacking Groups</td>
<td>Illegal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Criminal Organizations</td>
<td>Illegal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Terorist Organizations</td>
<td>Illegal</td>
</tr>
</tbody>
</table>
The effects of cyber action can occur on all layers of cyber space, in the physical and information environment, but the first (direct) consequences always occur on the logical layer of cyber space. They are not necessarily final. Due to the networking of objects and entities in cyberspace, the primary effects quickly induce the subsequent ones.

Provoking group or social instability and rebellion, election meddling, influence on consciousness, will and decision making process etc.

Neutralization, damage, destruction of systems, communications, infrastructure and connected entities
DragonflEye (GMO living being-machine-cyborg drone) with flight speed of 25 or 30 mph and solar power. Created by the Charles Stark Draper Laboratory and Howard Hughes Medical Center (Massachusetts, Virginia, U.S.) as a continuation of the Nano Hummingbird project backed by the Defense Advanced Research Projects Agency (DARPA).

What constitutes a cyber attack and the influence in relative future cases?
Offensive Cyber Capabilities (in international relations)

- Power projection
  - Cyber attack (harmful effects)
  - Cyber espionage
- Influence
  - Other forms of cyber aggression

Combination of different activities

I: 
- Availability
- Confidentiality
- Integrity
- Reliability
- Authenticity
- Non-repudiation

II: Physical Layer

III: Cognitive Layer

III: Physical Environment

Physical Layer

Cognitive Layer

Physical Environment
The participants in the conflict are the states that have joined the agreement that is the source of MHP. The conflict represents the use of force, armed force or aggression. IHL/LOAC and International Customary Law. Who are the participants of the conflict? The participants in the conflict are the states that have joined the agreement that is the source of MHP. The international character of the conflict. LOAC: *ius ad bellum, ius in bello*. War between at least two states. International armed conflict (are subject to Geneva Conventions and the Additional Protocol I). Non-international armed conflict (subject to the Article 3 of the Geneva Conventions and the Additional Protocol II). Other law systems. International customary (humanitarian) law: state practice *opinio juris*. National Law.
Technology Demands

State cyber defense capabilities

Attack Detection
Attacker Identification
Attacker Attribution
Response & React
Attack Prevention
**Application of Offensive Cyber Capabilities**

- **power projection**
- **influence**
  - by the use of adequate **means, techniques, methods**
  - to create **effects**
    - (of physical and non-physical nature)
  - in, through, and from cyberspace

**Cyber-attack**

- an attempt
- realization of an offensive activity
  - by the use of adequate **means, techniques, methods**
  - to create direct harmful **effects** in cyberspace
    - (logical layer)
  - physical and cognitive layer of cyberspace
  - physical and information environment
    - (outside of cyberspace)

---

**Cyber weapon**: system, such as software and hardware tool, strategically developed to deliver **power projection** in, through, and from cyberspace (Note: An ideal system is an absent system which performs the required function).

**Cyber aggression**: an attempt at or a process by a state in, through, or from cyberspace of causing **harm to sovereignty, territorial integrity or political independence** of another state, or in any other manner inconsistent with the objectives and provisions of the **UN Charter**.

**Cyber conflict**: an international conflict involving **use of offensive cyber capabilities** in cyberspace, with **harmful consequences** that manifest in, through, or from cyberspace.
Main characteristics

- OCCs are abilities for the planned and organized use of particular means, methods and tools (cyber weapons and cyber-attacks) to achieve effects and influence in, through, and from cyberspace
- They are always aggressive in nature, actively directed at the target
- Their first (direct) consequences happen at the logical layer of cyberspace
- The possibility, severity, and complexity of their use increases

Main challenges

- The application of IL is difficult in practice (lack of regulation and capabilities)
- Participants are mixed

Main recommendations

- Development of **new legal bodies** and instruments based on the experience of the existing law.
- Encouraging negotiations and agreements between the opposing sides, particularly at **bilateral** and UN levels.
- Initiating the process of creating an open, public and expert **methodology** for attacker attribution across the global multistakeholder community.