Defining Offensive Cyber Capabilities

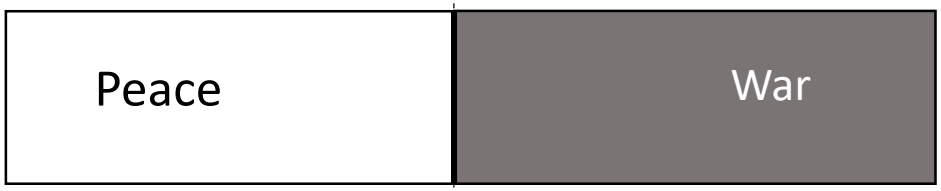
Diplo Foundation

Researchers:
Dragan Mladenović, Ph.D.
Vladimir Radunović

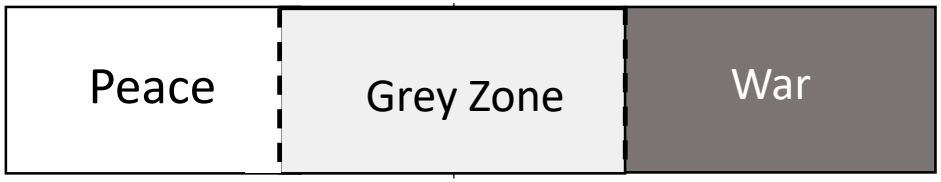
May 2018

Social Environment

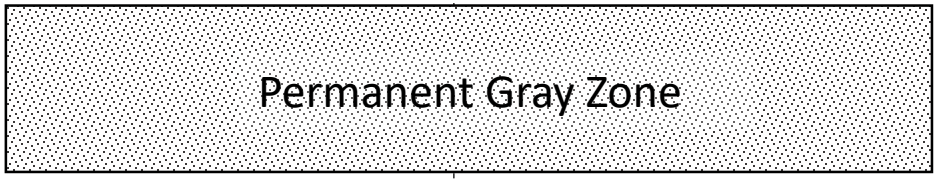
Conventional armed conflict of two belligerent sides
(Kende, 1971)



Cold war, internal and proxy wars
(van Creveld, 1991, 2001, 2006)



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)

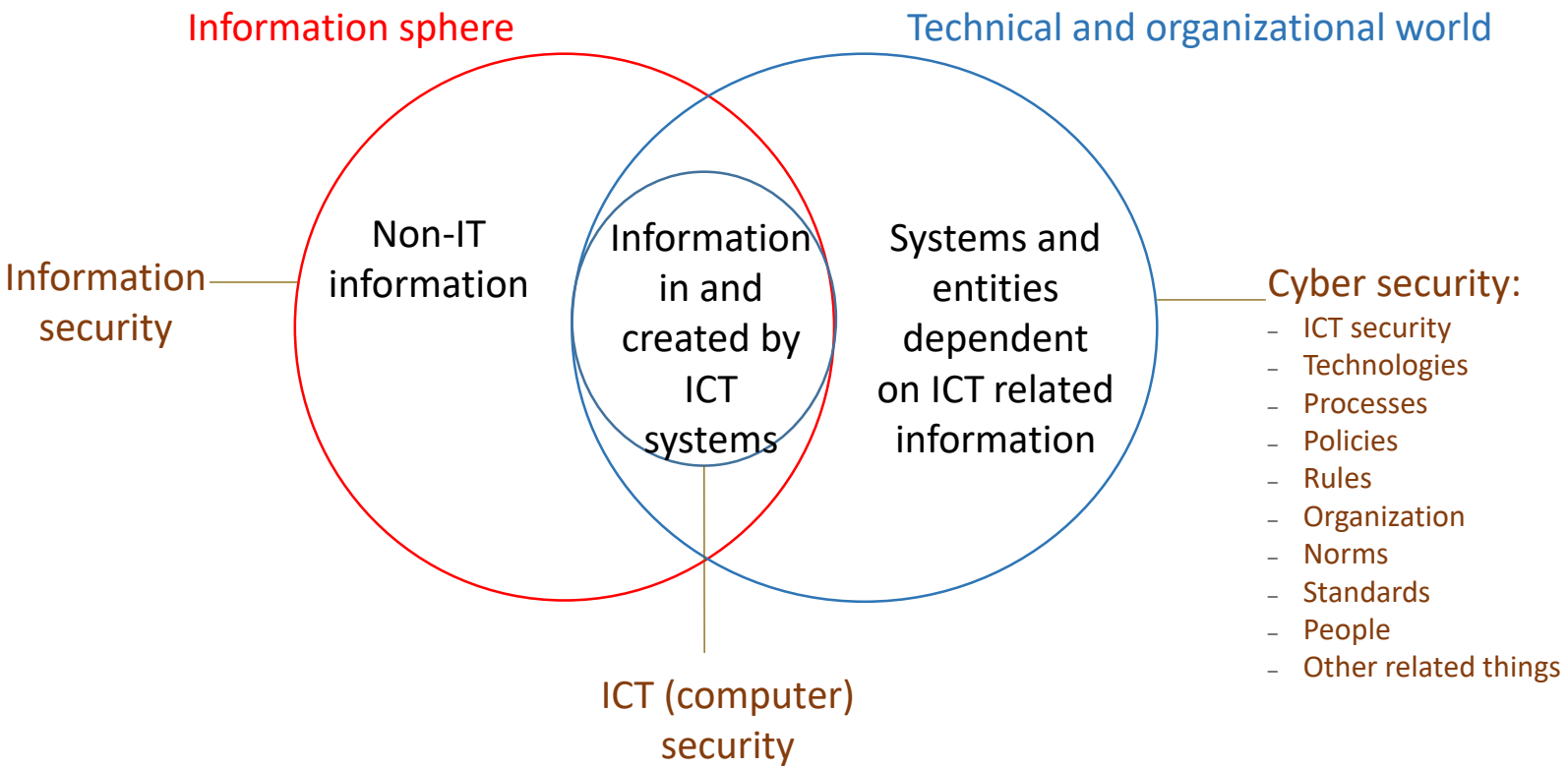


The traditional division of the period of armed conflict and peace is no longer applied in the practice of conflict, but it is applied in the practice of International Law .

“The saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom.” (Isaac Asimov, 1988).

Research Methodology and Professional Environment

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

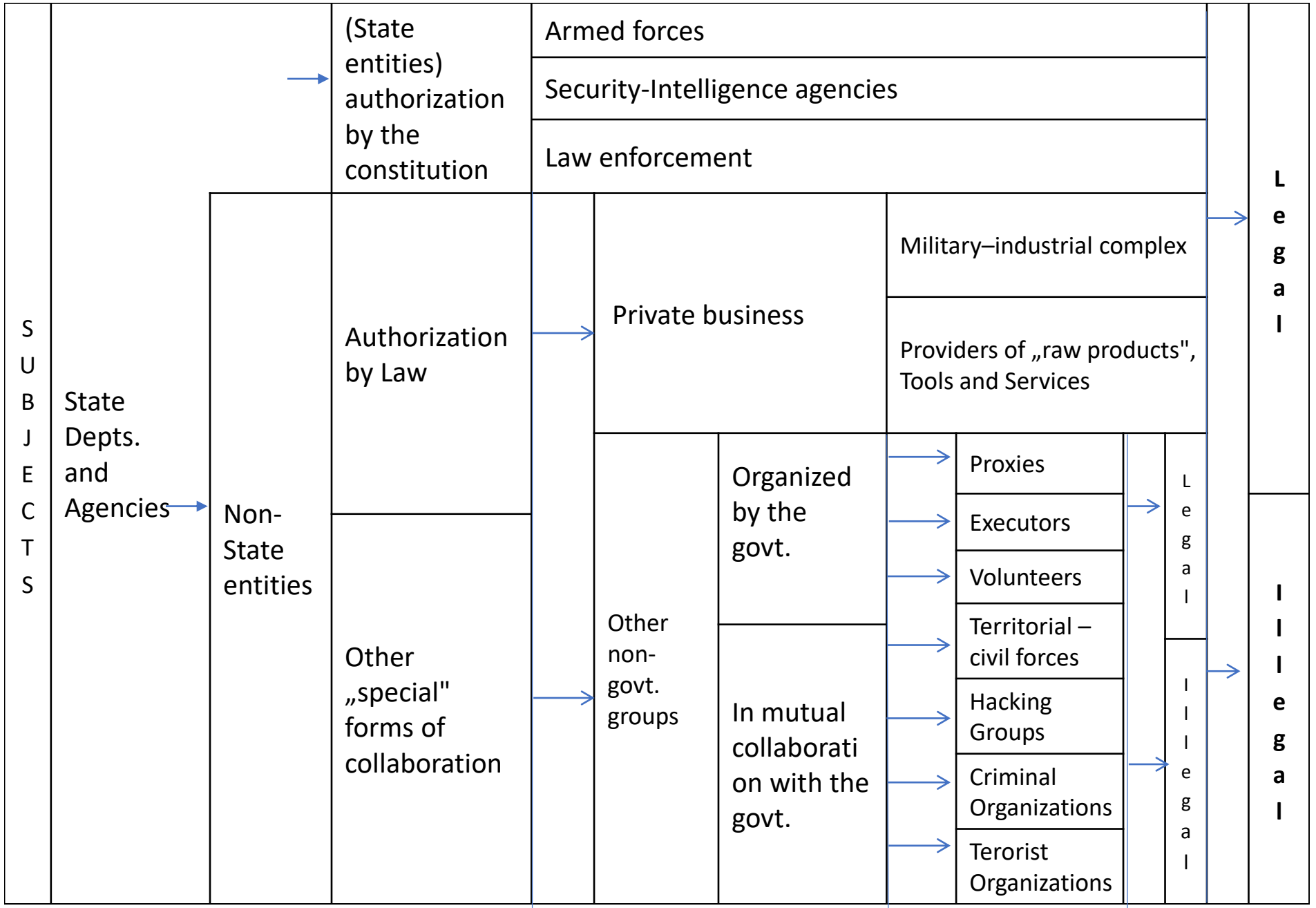


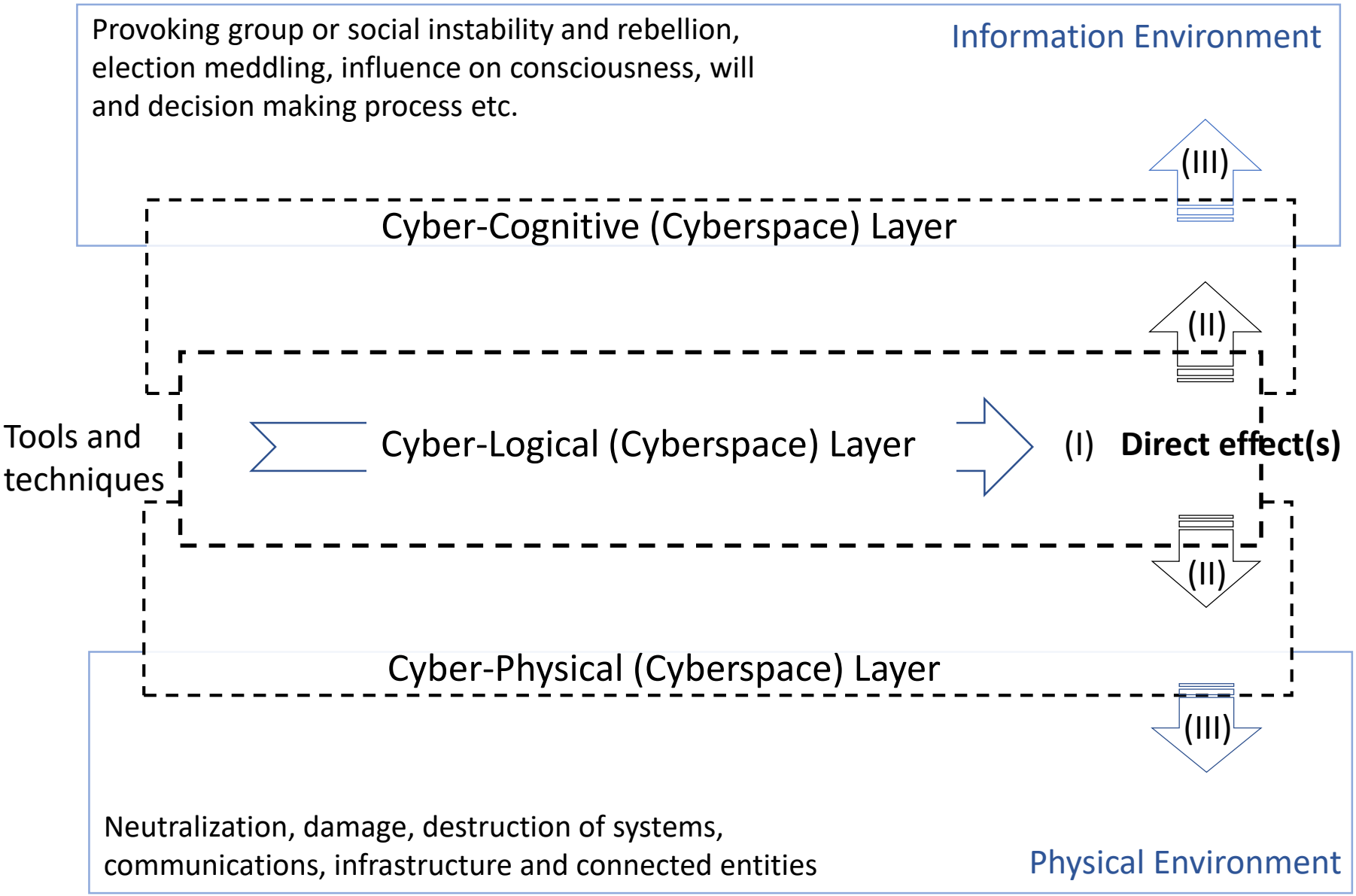
*Adapted from van Solms & van Niekerk

Offensive Cyber Capabilities

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

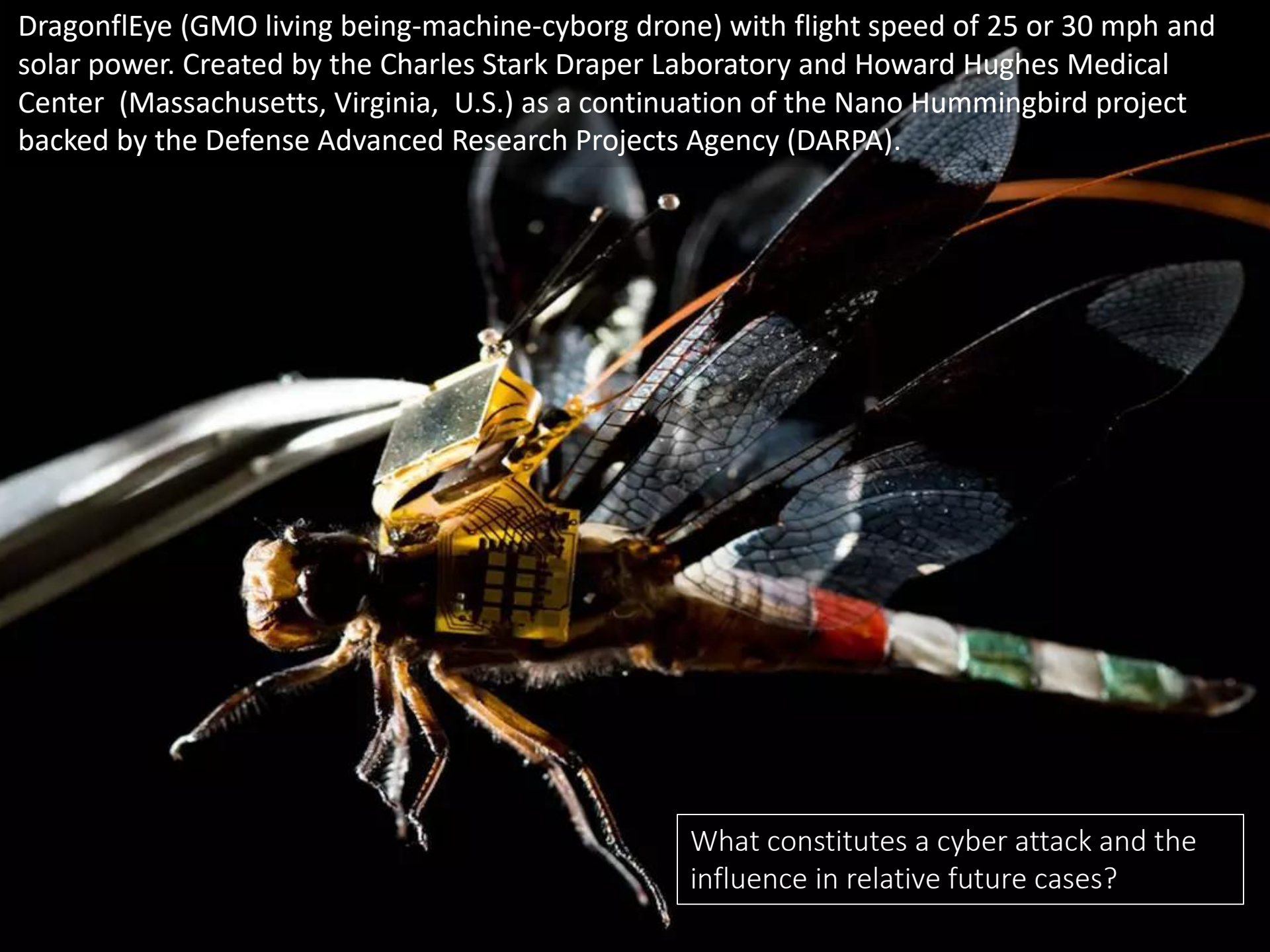
State Use of Offensive Cyber Capabilities



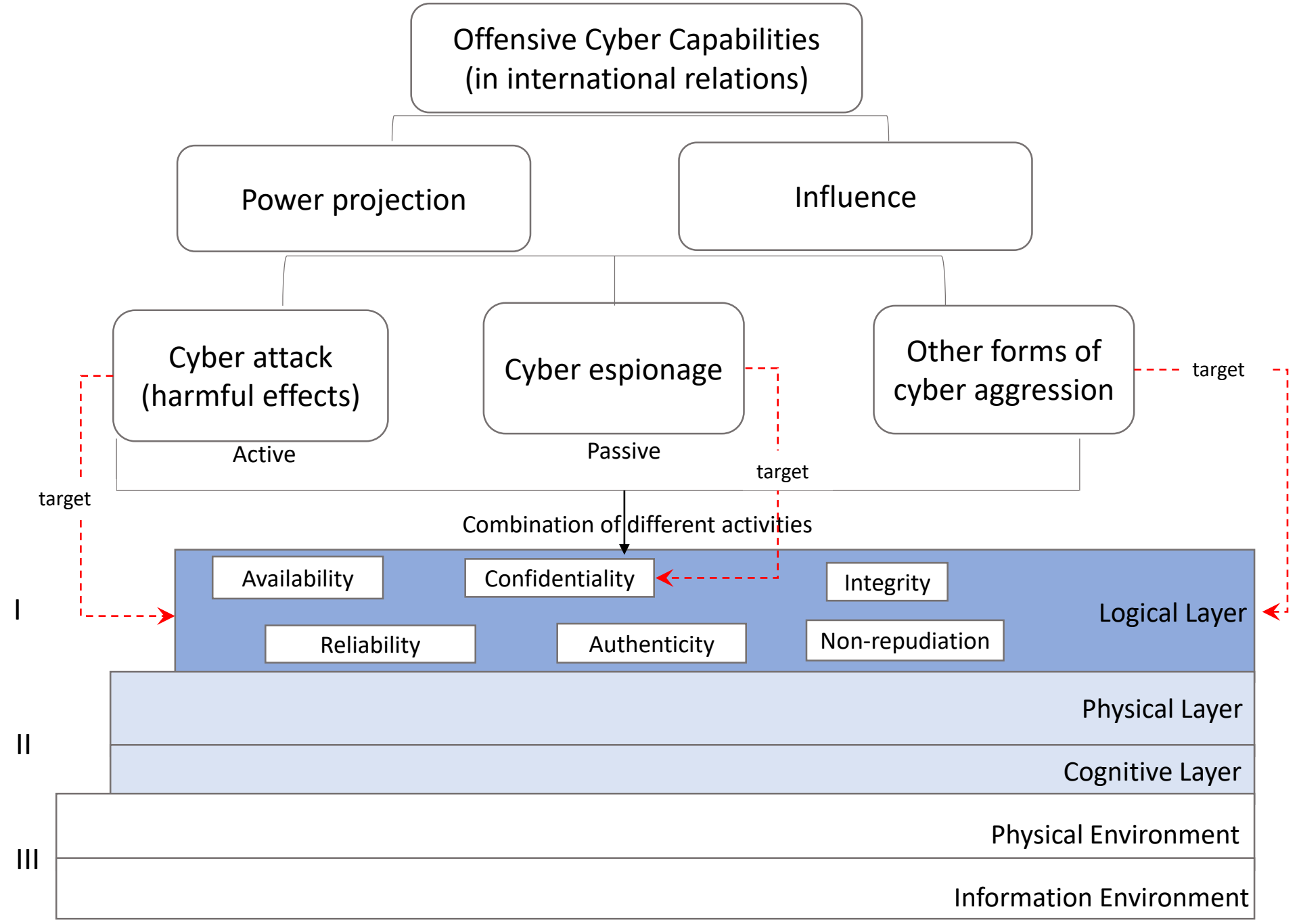


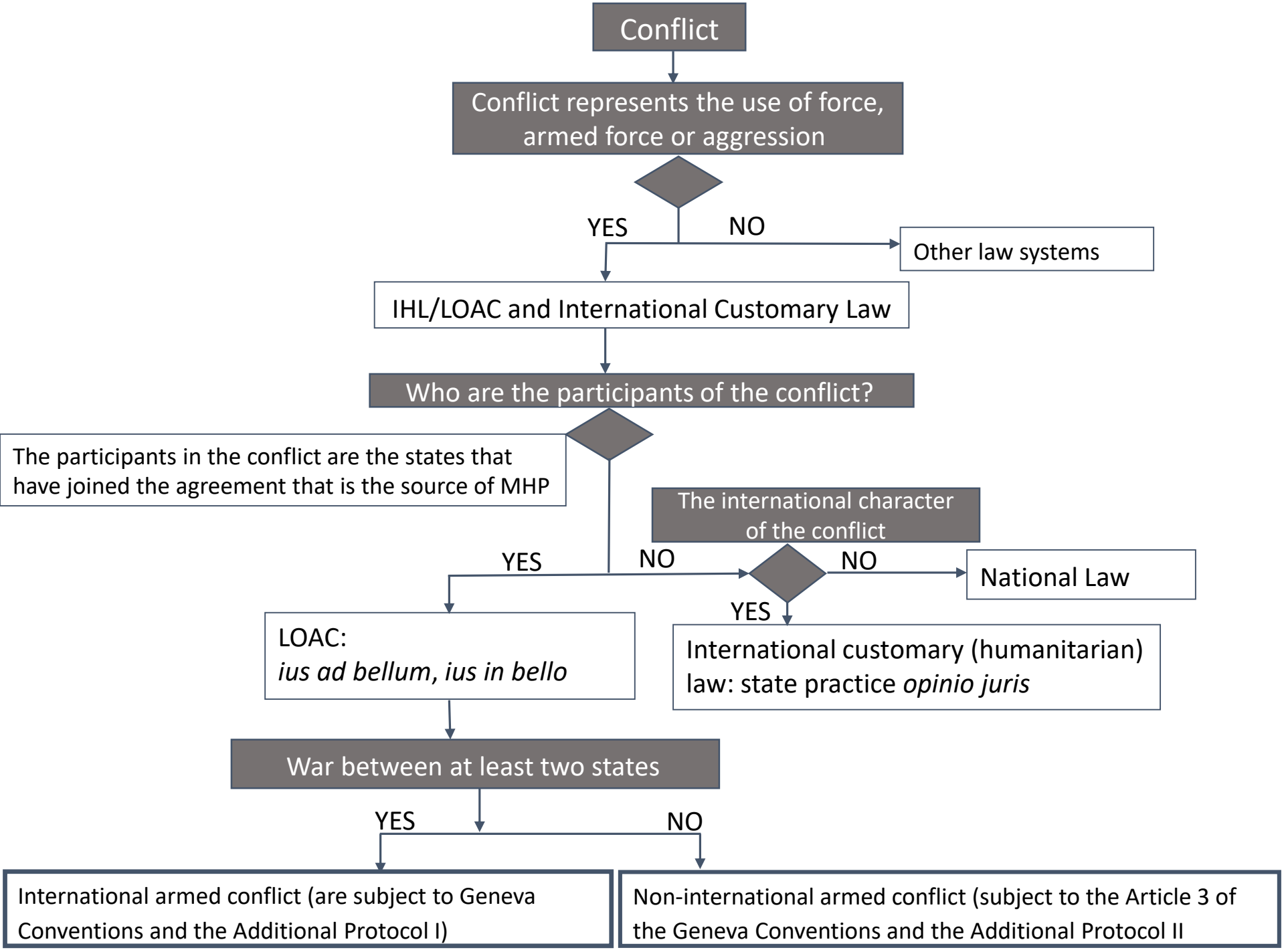
The effects of cyber action can occur on all layers of cyber space, in the physical and information environment, but the first (direct) consequences always occur on the logical layer of cyber space. They are not necessarily final. Due to the networking of objects and entities in cyberspace, the primary effects quickly induce the subsequent ones.

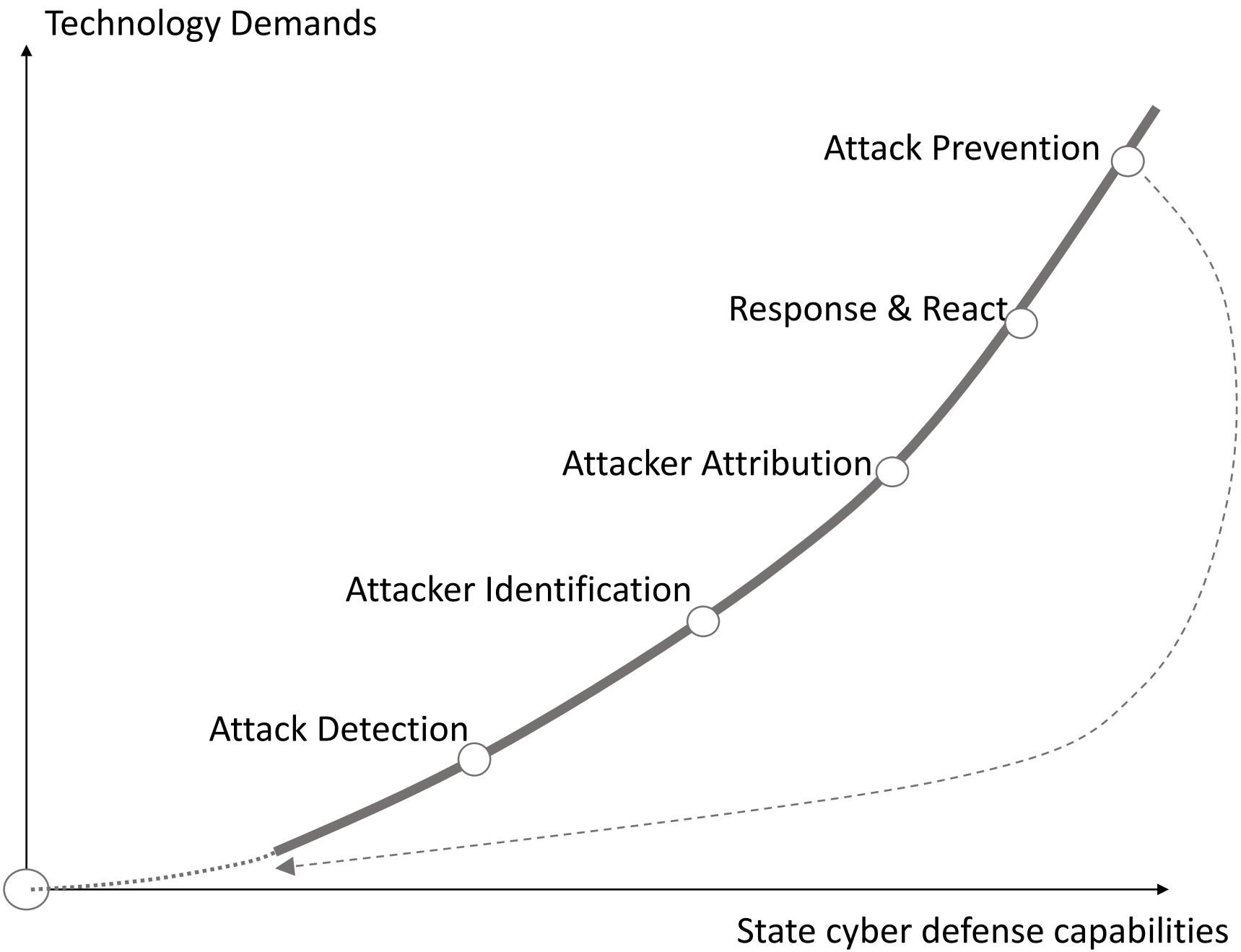
DragonflEye (GMO living being-machine-cyborg drone) with flight speed of 25 or 30 mph and solar power. Created by the Charles Stark Draper Laboratory and Howard Hughes Medical Center (Massachusetts, Virginia, U.S.) as a continuation of the Nano Hummingbird project backed by the Defense Advanced Research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



What constitutes a cyber attack and the influence in relative future cases?


Offensive Cyber Capabilities
(in international relations)
Power projection
Influence
Cyber attack
(harmful effects)
Cyber espionage
Other forms of
cyber aggression
Active
Passive
target
target
target
Combination of different activities
I
Availability
Confidentiality
Integrity
Reliability
Authenticity
Non-repudiation
Logical Layer
II
Physical Layer
Cognitive Layer
III
Physical Environment
Information Environment


Conflict
Conflict represents the use of force, armed force or aggression
YES
NO
Other law systems
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
YES
NO
NO
National Law
YES
LOAC:
ius ad bellum, ius in bello
International customary (humanitarian) law: state practice opinio juris
War between at least two states
YES
NO
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


Technology Demands
Attack Prevention
Response & React
Attacker Attribution
Attacker Identification
Attack Detection
State cyber defense capabilities

Definitions

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.

Conclusion and Recommendations

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.