



Multinational Experiment 7 Outcome 3 – Cyber Domain Objective 3.3

Addendum to Concept Framework

Version 3.0

03 October 2012

Distribution Statement

This document was developed and written by the contributing nations and organizations of the Multinational Experiment (MNE) 7. It does not necessarily reflect the views or opinions of any single nation or organization, but is intended as a guide. Reproduction of this document and unlimited distribution of copies is authorized for personal and non-commercial use only, provided that all copies retain the author attribution as specified below. The use of this work for commercial purposes is prohibited; its translation into other languages and adaptation/modification requires prior written permission. Questions or comments can be referred to MNE7_secretariat@apan.org.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 08 JUL 2013		2. REPORT TYPE N/A		3. DATES COVERED	
4. TITLE AND SUBTITLE Multinational Experiment 7 Outcome 3 - Cyber Domain Objective 3.3 Addendum to Concept Framework Version 3.0				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) JOINT STAFF-MN//ACT Integration 116 Lakeview Parkway Suffolk, VA 23435				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited.					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT Concept developers answers to major issues, concerning the International Law raised on by the Review/Clarification section of para 4.2 "Summary of Recommendations", within the LOE1 Analysis Report (AR) document - 20 July 2012.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 10	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Concept developers answers to major issues, concerning the International Law, raised on by the Review/Clarification section of para 4.2 “Summary of Recommendations”, within the LOE1 Analysis Report (AR) document - 20 July 2012.

LIST OF ANSWERED RECOMMENDATIONS

- 1. The definitions of the terms in the cells, especially for “cyber attack”, should be reviewed. A common understanding about these definitions is necessary and important.**
- 2. The CIAM should be reviewed to check whether cyber incidents could be legally assessed to be an “act of violence” at all.**
- 3. Use and definitions of the terms “use of force” and “armed force” should be reviewed and clarified.**
- 4. The definitions for the terms “cyber crime”, “cyber attack”, and “cyber war” should be reviewed and clarified. One option could be to use the definitions from the University of California.**
- 5. Concept developers should review the categories in the column “actor” regarding the distinction between the military and the state domain.**
- 6. Review the appropriateness of the term “terrorist” as a type of actor in CIAM.**

- 1. The definitions of the terms in the cells, especially for “cyber attack”, should be reviewed. A common understanding about these definitions is necessary and important.**

The definition of cyber attack remains inconsistent. Some commentators use the term to encompass a wide variety of acts of cyber terrorism and cyber warfare and other commentators use cyber attacks as a separate category.

There have been two particularly prominent government-led efforts to understand the scope of the threat posed by cyber-attacks, one by the U.S. government and the other by the Russia- and China-led Shanghai Cooperation Organization.

The U.S. National Research Council defines cyber-attack as “deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks.” Although the objective-based definitional approach taken by the United States is pretty clear, the complexity of these definitions fails to distinguish between a simple cyber-crime and a cyber-attack.

The Shanghai Cooperation Organization—a security cooperation group composed of China, Russia, and most of the former Soviet Central Asian republics, as well as observers—has adopted a much more expansive means-based approach to cyber-attacks. The Organization has “express[ed] concern about the threats posed by possible use of [new information and communication] technologies and means for the purposes incompatible with ensuring international security and stability in both civil and military sphere”.

NATO’s Strategic Concept and the 2010 Lisbon Summit Declaration recognize that “Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO’s permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO’s doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber attack against systems of critical importance to the Alliance” (para. 40).

However, the New Strategic Concept does not consider automatically cyber attacks as a threat justifying the use of force by the Alliance.

NATO art. 5 has a clear formulation, but what has to be considered is that an Art. 5 attack is decided on a case-by-case basis.

2. The CIAM should be reviewed to check whether cyber incidents could be legally assessed to be an “act of violence” at all.

As to the definition of “act of violence”, Art. 49(1) of the Additional Protocol I of Geneva Conventions 1949, provides that “Attack means acts of violence against the adversary, whether in offence or in defense”. This definition has triggered significant discussion as to what extent cyber operations, in view of their non- kinetic nature, could be regarded as “acts of violence” and, therefore, as “attacks” within the meaning of International Humanitarian Law.

Today, it seems to be generally recognized that “acts of violence” do not necessarily require the use of kinetic violence, but that it is sufficient if the resulting effects are equivalent to those normally associated with kinetic violence, namely the death or injury of persons or the physical destruction of objects (effects-based approach).

Strictly speaking, this approach does not “extend” the notion of attack beyond acts of violence, but simply recognizes that cyber operations triggering processes likely to directly cause death, injury or destruction are not only equivalent to, but constitute an integral part of, an “act of violence” within the meaning of article 49(1) of AP I.

There is disagreement, however, as to whether the notion of attack also includes cyber operations aiming to merely capture or neutralize (that is, inhibit, hinder or hamper the proper exercise of its function)—rather than kill, injure or destroy—the target. The leading argument in favour of extending the effects-based interpretation of “attack” to cyber operations aiming to “neutralize” is that the treaty definition of military objectives in article 52(2) of AP I includes objects whose “capture and neutralization” would offer a definite military advantage and puts these two alternatives on the same level as total or partial destruction. Those opposing this extension base themselves on a more literal interpretation of attacks as “acts of violence” and require that, if not the act itself, at least its consequences must be violent in order for it to be considered as an attack. In support of their view they further point out that the principle of proportionality is formulated in terms of attacks causing “loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof”¹¹⁵ but does not include capture or neutralization.

The term “act of violence” is presently related to:

- 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (*Civil Aviation Convention*) which makes it an offence for any person unlawfully and intentionally to perform an act of violence against a person on board an aircraft in flight, if that act is likely to endanger the safety of the aircraft; to place an explosive device on an aircraft; to attempt such acts; or to be an accomplice of a person who performs or attempts to perform such acts;
- 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation;
- 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (*Maritime Convention*) which establishes a legal regime applicable to acts against international maritime navigation that is similar to the regimes established for international aviation and makes it an offence for a person unlawfully and intentionally to seize or exercise control over a ship by force, threat, or intimidation; to perform an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of the ship; to place a destructive device or substance aboard a ship; and other acts against the safety of ships.

Those instruments were developed under the auspices of the United Nations and its specialized agencies and the International Atomic Energy Agency and are open to participation by all Member States. In 2005, the international community also introduced substantive changes to three of these universal instruments to specifically account for the threat of terrorism.

3. Use and definitions of the terms “use of force” and “armed force” should be reviewed and clarified.

“Armed attack” is, although closely related, a narrower category than “threat or use of force. The dominant view in the United States and among its major allies has long been that the Article 2(4) prohibition of force and the complementary Article 51 right of self-defence apply to military attacks or armed violence. As noted, “term *force* as used in Article 2(4) is according to the correct and prevailing view, limited to armed force”.

The plain meaning of the text supports this view, as do other structural aspects of the U.N. Charter. For example, the Charter’s preamble sets out the goal that “*armed* force . . . not be used save in the common interest.” Similarly, Articles 41 and 42 authorize, respectively, the Security Council to take actions not involving armed force and, should those measures be inadequate, to escalate to armed force.

However, there are textual counter-arguments, such as that Article 51’s more specific limit to “armed attacks” suggests that drafters envisioned prohibited “force” as a broader category not limited to particular methods.

The existence of a loophole between art. 2(4) and 51 of the UN Charter is confirmed by art. 3 of the GA Resolution no.3314/74 (XXIX) on the definition of aggression (which is now the content of art. 8 bis par. 2 of Rome Statute of the ICC according to the resolution RC/RES.6 , 11 June 2010) trying to link art.2(4), and art.51 of the UN Chart.

On the one hand, the resolution confirms the will to consider as aggression just the “armed force”, excluding all the situations related to economic or political attacks; on the other hand, the resolution clarifies that the only aggression justifying self-defence is the armed one.

However, the list provided by art 3 shows the characteristics common to all the types of aggression which is a use of force “on a relatively large scale and with substantial effects”; this feature begs for the conclusion that the scope of “armed attack” doesn’t exactly correspond to that of “use of force”.

Although the provisions of the resolutions are not binding as UN GA resolution, its ability to strengthen the argument that there is a gap between art 2(4) and art 51 is also reflected by the ICJ judgment in Nicaragua case (ICJ, 1986). In *Nicaragua* case, the ICJ, also failing to define “armed attack”, expressly affirmed that the use of force could be divided into two categories, “most grave” (those constituting armed attacks) and “less grave”, giving the word “force” at art. 2 (4) a broader meaning than art. 51.

4. **The definitions for the terms “cyber crime”, “cyber attack”, and “cyber war” should be reviewed and clarified. One option could be to use the definitions from the University of California.**

Cyber-crime is a broad concept analytically distinct from cyber-attack. While, as with the concept of cyber attack, there is no universally recognized definition of cyber-crime, there are aspects of cyber-crime that are broadly recognized. Cyber-crime is generally understood as the use of a computer-based means to commit an illegal act.

One typical definition describes cyber-crime as “*any crime that is facilitated or committed using a computer, network, or hardware device.*” and is activity conducted for profit, primarily motivated by financial gain or notoriety.

Cyber crime typically involves the production of malware, the distribution of child pornography, hijacking for ransom, the sale of mercenary services, and the like.

Cyber-crimes need not undermine the target computer network (though in some cases they may do so), and most do not have a political or national security purpose. Finally, like all crimes, but unlike cyber-attacks, cyber-crimes are generally understood to be committed by individuals, not states.

An act is only a cyber-crime when a non-state actor commits an act that is criminalized under state or international law. Most cyber-crimes do not also constitute cyber-attack or cyber-warfare.

Cyber-crime committed by a non-state actor for a political or national security purpose is a cyber-attack. On the other hand, cyber-crime that is not carried out for a political or national security purpose, such as Internet fraud, identity theft, and intellectual property piracy, does not fit this final element of a “cyber-attack” and is therefore mere cyber-crime.

As to Cyber-warfare and cyber-war, they are substantially synonymous. According to CCDCOE cyber warfare is “an activity related to enhancement of the battle space awareness or force application which occurs in, or performed from or uses cyberspace”. In that context cyber-warfare seems to be broader than cyber-war.

Cyber-warfare is distinctive among the three cyber-categories considered here in that cyber-warfare *must* also constitute a cyber-attack. When a cyber-attack constitutes an armed attack, it can be accurately considered “cyber-warfare.”

According with the University of California (see A. Hathaway, Rebecca Crotoff, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel in “The Law of Cyber attacks”, California Law Review, 2012 at 18- UNIVERSITY OF CALIFORNIA), a cyber-attack consists of *any action taken to undermine the functions of a computer network for a political or national security purpose.*

A cyber-attack’s means can include *any* action—hacking, bombing, cutting, infecting, and so forth—but the objective can only be to undermine or disrupt the function of a computer network. The objective of a cyber-attack must be to undermine the *function* of a computer network.

Mere cyber-espionage, or cyber-exploitation, does not constitute a cyber-attack, because neither of these concepts involves altering computer networks in a way that affects their current or future ability to function. To “undermine the function” of a computer system, an actor must *do more than passively observe a computer network or copying data*, even if that observation is clandestine. Such activities may be criminal—as acts of corporate or political cyber-espionage—but are not cyber-attacks. In this respect, our definition reflects a common distinction between espionage and attacks in more traditional settings.

A political or national security purpose distinguishes cyber-attack from simple cyber-crime. Any aggressive action taken by a state actor in the cyber-domain necessarily implicates national security and is therefore a cyber-attack (where the action satisfies all the other elements of the definition), whether or not it rises to the level of cyber-warfare.

Essential Characteristics of Different Cyber-Actions, Type Of Cyber-Action.	Involves only non-state actors.	Must be violation of criminal law, committed by means of a computer system.	Objective must be to undermine the function of a computer network.	Must have a political or national security purpose.	Effects must be equivalent to an “armed attack,” or activity must occur in the context of armed conflict.
Cyber-Attack			X	X	
Cyber-Crime	X	X			
Cyber-Warfare			X	X	X

5. Concept developers should review the categories in the column “actor” regarding the distinction between the military and the state domain.

According to art. 4 Draft Articles on State Responsibility for Internationally Wrongful Acts:

“1.The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State.

2.An organ includes any person or entity which has that status in accordance with the internal law of the State”.

As a consequence, an act carried out by militaries, considered as an effective organ of the State, should be considered as an act of State. No substantial difference exists therefore between a State or Military act when the military organ at issue exercises control over or directs the political or military action of a State and so there is a direct link between the military decision and the State will.

Any military act as provided by art. 8bis par. 2 is automatically considered as an act of State which expressly make reference to "The use of armed forces of one State ".

The whole of art. 8bis para. 2 shows a direct link between armed forces and the State, as they represent, directly or indirectly its will and so their acts, in the limits of the above, are directly linked to the State.

UNCLASSIFIED

Finally, under the definition provided at par.1, the crime of aggression is committed “by a person in a position effectively to exercise control over or to direct the political or military action of a State.”

Thus, the crime is solely a “leadership crime.” Although military, ordinary soldiers would never be covered by the definition. This understanding is confirmed as well by the amendment to Rome Statute Article 25, also agreed to at the Review Conference, which would insert into Article 25, a paragraph 3bis stating: “In respect of the crime of aggression, the provisions of this article shall apply only to persons in a position effectively to exercise control over or to direct the political or military action of a State.”

Unlike State armed forces, however, private military personnel occupy a relatively ambiguous legal status. One often hears the employees of private military companies being referred to as “mercenaries”.

While the definition of mercenaries is similar in the International Convention against the Recruitment, Use, Financing and Training of Mercenaries, the then Organization of African Unity Convention for the Elimination of Mercenarism in Africa (together known as “the mercenary conventions”) and under Additional Protocol I of the Geneva Convention, the consequence of being deemed to be a mercenary is different.

Since the mercenary conventions adopt a definition of mercenaries similar to that established in Article 47 of Protocol I, we can use that definition as our starting point. Article 47.2 of Additional Protocol I stipulates, a mercenary is any person who:

- a. is specially recruited locally or abroad in order to fight in an armed conflict;
- b. does, in fact, take a direct part in the hostilities;
- c. is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party;
- d. is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict;
- e. is not a member of the armed forces of a Party to the conflict; and (f) has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces.

The definition in Article 47 is widely viewed as being virtually “unworkable” owing to the six cumulative conditions that a person must fulfill in order to be considered a mercenary.

Without a clear working definition, the problem arises of how to ensure states comply with international laws relating to the control mercenaries and their liability of their acts.

The international community recognized the need for a multilateral convention.

During the course of the thirty-fifth session of the General Assembly it was therefore decided to draft an International Convention against the recruitment, use, financing and training of mercenaries. The Convention was presented to the General Assembly for signature and ratification in December 1989. The Convention adopts a more inclusive definition than that found in the Additional Protocol I. As a result, the recruitment, use, financing and training of mercenaries are also declared to be offences.

Since 1989, when the Convention against the Recruitment, Use, Financing and Training of Mercenaries was signed, The United Nations General Assembly has continued to pass

resolutions concerned with the activities of mercenaries. Such resolutions, as previously explained, have, in general, reflected the restricted nature of the ban on the use of mercenaries, as well as those traditional worries expressed by the international community towards the activity of individuals engaged in mercenary activities, while also dealing with the actions of mercenaries in a variety of different circumstances. In the case of mercenaries, although military force, it is questionable if their acts can be attributable to the State for its lack of control.

In other cases, the problem is linked to the already pointed out question of the accountability for cyber acts to the State.

6. Review the appropriateness of the term “terrorist” as a type of actor in CIAM

International law lacks a general definition of "terrorist". The various sector counter-terrorism conventions define and criminalize particular categories of terrorist activities, providing an indirect definition of "terrorist":

- a. Article 2.1 of the 1997 International Convention for the Suppression of Terrorist Bombings indirectly defines as a terrorist "Any person [...that] unlawfully and intentionally delivers, places, discharges or detonates an explosive or other lethal device in, into or against a place or public use, a State or government facility, a public transportation system or an infrastructure facility:
 - (1) With the intent to cause death or serious bodily injury; or
 - (2) With the intent to cause extensive destruction of such a place, facility or system, where such a destruction results in or is likely to result in major economic loss."
- b. Article 19 expressly excluded from the scope of the convention certain activities of state armed forces and of self-determination movements.
- c. Article 2.1 of the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention) indirectly defines a terrorist as "any person" who "by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an act "intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."

The 2005 United Nations International Convention for the Suppression of Acts of Nuclear Terrorism provides at art.2 "1. Any person commits an offence within the meaning of this Convention if that person unlawfully and intentionally:

- a. Possesses radioactive material or makes or possesses a device:
 - (i) With the intent to cause death or serious bodily injury; or
 - (ii) With the intent to cause substantial damage to property or to the environment;
- b. Uses in any way radioactive material or a device, or uses or damages a nuclear facility in a manner which releases or risks the release of radioactive material:
 - (i) With the intent to cause death or serious bodily injury; or
 - (ii) With the intent to cause substantial damage to property or to the environment; or
 - (iii) With the intent to compel a natural or legal person, an international organization or a State to do or refrain from doing an act".

UNCLASSIFIED

In the context of the EU, the most important documents have been the Common Position 2001/931/CFSP of 27 December 2001¹⁵ and the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism. These documents set out a series of measures but, more importantly, they are the first documents providing solid criteria for the definition of terrorists and terrorist groups.

According to these definitions there are three basic criteria to be employed in order to characterize a group or an act as terrorist:

- a. **The acts:** Both the Common Position and the Council Decision refer to a series of criminal acts that will be deemed as terrorist offences.
- b. **The aim:** According to both the Common position and the Council Decision, the above acts, in order to constitute terrorist offences, must be committed with the intention of (i) seriously intimidating a population, (ii) compelling a government or international organization to perform or abstain from performing any act or (iii) seriously destabilizing or destroying the fundamental political, constitutional or social structures of a state or international organization.
- c. **Participation in a terrorist organization:** The 2001 Common Position lists offences relating to the participation in a terrorist group among the acts considered as terrorist. On the contrary, the 2002 Council Decision creates a separate category of offences for direction of or participation in a terrorist group or financing such activities and obliges member states to introduce separate legislation for the punishment of such activity.

Whereas the 2001 Common Position does not make any kind of distinction between the groups that would perform terrorist acts, the 2002 Framework Decision, in para. 11 of its preamble specifically states “... *actions by the armed forces of a State in the exercise of their official duties are not governed by this Framework Decision*”, thus following the idea that the notion of terrorism should be confined to the activities of private groups and cannot, under any circumstances, include actions by state organs or official state policies, even if they match the abovementioned criteria.