XIII Seminario online

ACDIA
Asociación de Colegios
de Defensa Iberoamericanos

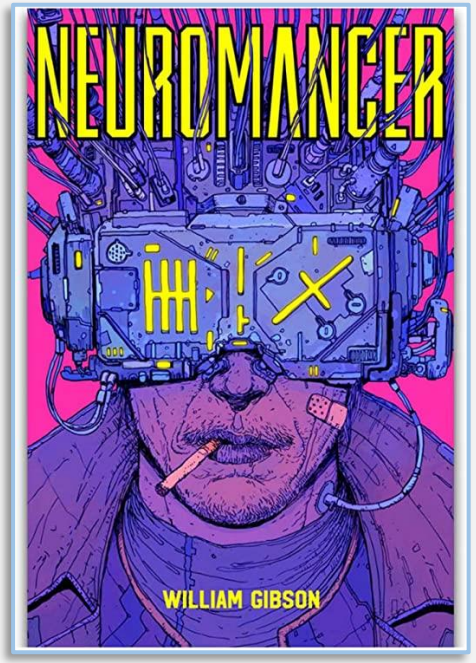
CESNAV
Centro de Estudios
Superiores Navales

Operaciones Militares en el Ciberespacio y Derecho Internacional

20 DE MARZO DE 2024

General Auditor Jerónimo Domínguez Bascoy
Centro Superior de Estudios de la Defensa Nacional
(CESEDEN)

Primera aparición del término **"Ciberespacio"** en una obra del género "cyberpunk" (***Neuromancer***, W. Gibson, 1984): **red de ordenadores interconectados que une a personas y máquinas en una suerte de realidad virtual**.



To **many of us**, **cyberspace** is the **virtual world we experience when we go online to communicate, work and conduct everyday tasks**. In **technical terms**, cyberspace is the **interdependent network of information technology that includes the internet, telecommunications networks, computer systems and internet connected devices**. For the **military**, and when considering our efforts to counter threats in cyberspace, it is **an operational domain**, along with land, sea, air and space.

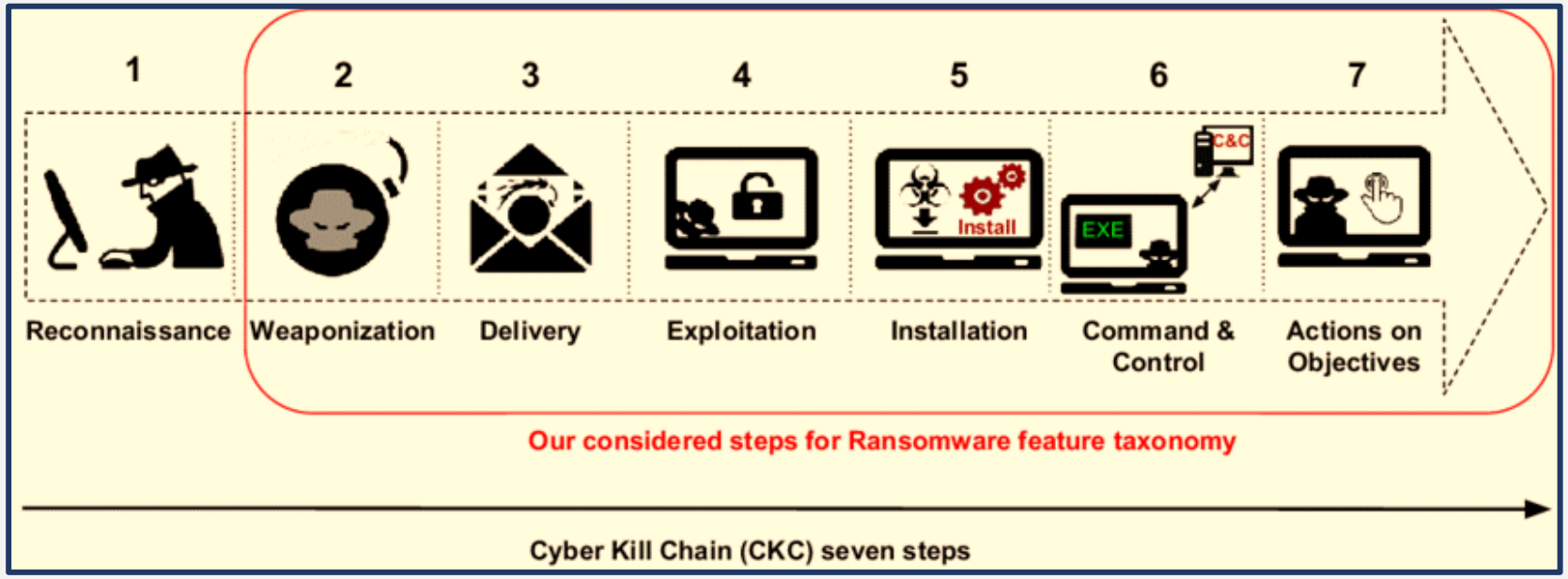
HM Government

National Cyber Strategy 2022

Pioneering a cyber future with the whole of the UK

Ciberoperaciones: Actividades en las que se emplean **capacidades cibernéticas** para alcanzar **objetivos** en o a través del **ciberespacio.**

Ciberataque: Cuando se compromete la **disponibilidad, integridad y confidencialidad** de la información mediante el **acceso no autorizado**, la **modificación**, **degradación** o **destrucción** de los **sistemas** de información y telecomunicaciones o de las **infraestructuras** que soportan.



El Ciberespacio: nuevo dominio militar (EEUU)

El Estado Mayor Conjunto, en su **Estrategia Militar Nacional** de **2004**, declaró que el ciberespacio era un "dominio" de conflicto junto con el aéreo, el terrestre, el marítimo y el espacial, y señaló que el Departamento de Defensa debía mantener su capacidad para defenderse y enfrentarse a los actores enemigos en este nuevo dominio.

El **21 de mayo de 2010**, el **US Cyber Command**, nacido de la fusión de la "JTF– Global Network Operations" y del "Joint Functional Component Command – Network Warfare" alcanzó su **Capacidad Operativa Inicial**. El USCYBERCOM quedó **dentro de la organización del Mando Estratégico** de los Estados Unidos (USSTRATCOM)

En **2018**, el presidente Donald Trump ordenó su elevación a **Mando Unificado de Combate**.

El Ciberespacio: nuevo dominio militar (España)

- Enero de 2011: aprobación por el JEMAD de la **"Visión de la Ciberdefensa Militar"**.
- Julio de 2011: aprobación por el JEMAD del **"Concepto de Ciberdefensa Militar"**.
- Julio de 2012: aprobación por el JEMAD del **"Plan de Acción para la Obtención de la Capacidad de Ciberdefensa Militar"**.
- **Febrero de 2013**: Orden Ministerial 10/2013, por la que se crea el **"Mando Conjunto de Ciberdefensa"**.
- Septiembre de 2015: creación en el EMAD de la **Jefatura de Sistemas de Información y Telecomunicaciones** (JCISFAS), heredera de la División CIS del EMACON, con la responsabilidad de elaborar los requerimientos de los Sistemas de Información y Telecomunicaciones de la estructura operativa de las FAS, incluyendo los Sistemas de Guerra Electrónica (EW) y de Observación de la Tierra (SOT).
- **Julio 2020**: la Orden DEF/710/2020 determina que en el ámbito ciberespacial debe garantizarse la necesaria libertad de acción de las FAS. A tal efecto, se ha creado el **"Mando Conjunto del Ciberespacio"** para reforzar la capacidad de actuación de éstas en dicho ámbito. Este Mando se establece sobre la base del Mando Conjunto de Ciberdefensa (MCCD) y de la Jefatura de Sistemas de Información y Telecomunicaciones (JCISFAS), que desaparecen de la nueva estructura del Estado Mayor de la Defensa.

El Ciberespacio: nuevo dominio militar (España)

[…] la transición de un modelo de ciberseguridad de carácter **preventivo y defensivo** hacia un esquema que incorpore elementos de **mayor fuerza disuasoria** obedece a un contexto global de mayor competencia geopolítica. El **empleo del ciberespacio como dominio de confrontación**, de forma independiente o como parte de una acción híbrida, es un rasgo ampliamente reconocido. La disuasión en ciberseguridad requiere la obtención y potenciación de **capacidades de ciberdefensa**, como elemento fundamental de la acción del Estado.

[España] abogará por la creación de un **marco internacional para la prevención de conflictos**, la cooperación y la estabilidad en el ciberespacio, en el que se apliquen los principios de la Carta de Naciones Unidas en su totalidad, el **Derecho Internacional**, los Derechos Humanos y el Derecho Humanitario Bélico, así como las **normas no vinculantes sobre el comportamiento responsable** de los Estados.

El Ciberespacio: nuevo dominio militar (OTAN)

Warsaw Summit Communiqué

Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council

70. Cyber attacks present a clear **challenge to the security** of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and **recognise cyberspace as a domain of operations** in which NATO must defend itself as effectively as it does in the air, on land, and at sea. […]. We reaffirm our commitment to act in accordance with **international law**, including the UN Charter, international humanitarian law, and human rights law, as applicable. We will continue to follow the principle of restraint and support maintaining international peace, security, and stability in cyberspace. We welcome the work on voluntary international **norms of responsible state behaviour** and confidence-building measures regarding cyberspace.

El Ciberespacio: nuevo dominio militar (UE)

Consejo de la Unión Europea

Bruselas, 19 de noviembre de 2018
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
Fecha:	19 de noviembre de 2018
A:	Delegaciones
Asunto:	Marco político de ciberdefensa de la UE (actualización de 2018)

En el anexo se remite, a la atención de las delegaciones, el marco político de ciberdefensa de la UE (actualización de 2018), adoptado por el Consejo en su sesión n.° 3652 celebrada el 19 de noviembre de 2018.

ANEXO

MARCO POLÍTICO DE CIBERDEFENSA DE LA UE

(según actualización de 2018)

Ámbito de aplicación y objetivos

Para responder a los retos cambiantes en el ámbito de la seguridad, la UE y sus Estados miembros deben reforzar la ciberresiliencia y desarrollar capacidades sólidas en ciberseguridad y defensa.

El marco político de ciberdefensa de la UE apoya el desarrollo de las capacidades en ciberdefensa de los Estados miembros de la UE y el refuerzo de la ciberprotección de la infraestructura de seguridad y defensa de la UE, sin perjuicio de la legislación nacional de los Estados miembros y de la UE, incluido el ámbito de aplicación de la ciberdefensa, si está definido.

El ciberespacio es el quinto ámbito de actuación, junto con los ámbitos de tierra, mar, aire y espacio. La ejecución exitosa de las misiones y operaciones de la UE depende cada vez más del acceso ininterrumpido a un ciberespacio seguro y ello requiere unas capacidades operativas sólidas y resilientes en el ámbito cibernético.

El Ciberespacio: nuevo dominio militar (UE)

COMISIÓN EUROPEA

ALTO REPRESENTANTE DE LA UNIÓN PARA ASUNTOS EXTERIORES Y POLÍTICA DE SEGURIDAD

Bruselas, 16.12.2020
JOIN(2020) 18 final

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO

La Estrategia de Ciberseguridad de la UE para la Década Digital

En 2018, la EU identificó el ciberespacio como un dominio de operaciones. Una próxima **«Visión y estrategia militar en el ciberespacio como un dominio de operaciones»** desarrollada por el Comité Militar de la UE debería definir aún más cómo el ciberespacio como dominio de operaciones permite que se realicen las misiones y operaciones militares de la PCSD de la UE.

La UE continúa trabajando con sus socios internacionales para avanzar y **promover un ciberespacio global, abierto, estable y seguro en el que se respete el derecho internacional**, en concreto la Carta de las Naciones Unidas, y se cumplan las normas voluntarias, reglas y principios de conducta responsable de los Estados. […] La UE es la más indicada para avanzar, coordinar y consolidar las posturas de los Estados miembros en los foros internacionales y debe desarrollar una **postura de la UE sobre la aplicación del derecho internacional en el ciberespacio**.

El Ciberespacio: nuevo dominio militar (UE)

EEAS(2021) 706 REV4
LIMITE
Releasable to NATO IMS and NATO Command Structure

European Union
EXTERNAL ACTION

European Union Military Staff

Official document of the European External Action Service of 15/09/2021

EEAS Reference	**EEAS(2021) 706 REV4**
Distribution marking/ Classification	**LIMITE**
From **To**	**European Union Military Staff (EUMS)** **European Union Military Committee (EUMC)** **CSDP/PSDC; EUMC**
Title / Subject	**European Union Military Vision and Strategy on Cyberspace as a Domain of Operations**
[Ref. prev. doc.]	

VISION *(ENDS)*

31. Ahead of all other considerations, the international law, including the UN Charter in its entirety, international humanitarian law, international human rights law, and the law of armed conflict apply in cyberspace. In that regard, these laws and the established principles of necessity, distinction and proportionality bind all EU CSDP military operations and missions stakeholders. Furthermore, commanders are to conduct any action in cyberspace in accordance with the operation mandate, and under commonly agreed Rules of Engagement (RoE).

El Ciberespacio: nuevo dominio militar (ONU)

DISEC
COMITÉ DE DESARME
Y SEGURIDAD INTERNACIONAL

United Nations A/AC.290/2021/CRP.2

General Assembly

Conference room paper
10 March 2021

English only

Open-ended working group on developments in the field of information and telecommunications in the context of international security

United Nations A/76/135

General Assembly

Distr.: General
14 July 2021

Original: English

Seventy-sixth session
Item 96 of the preliminary list*
Developments in the field of information and telecommunications in the context of international security

Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security

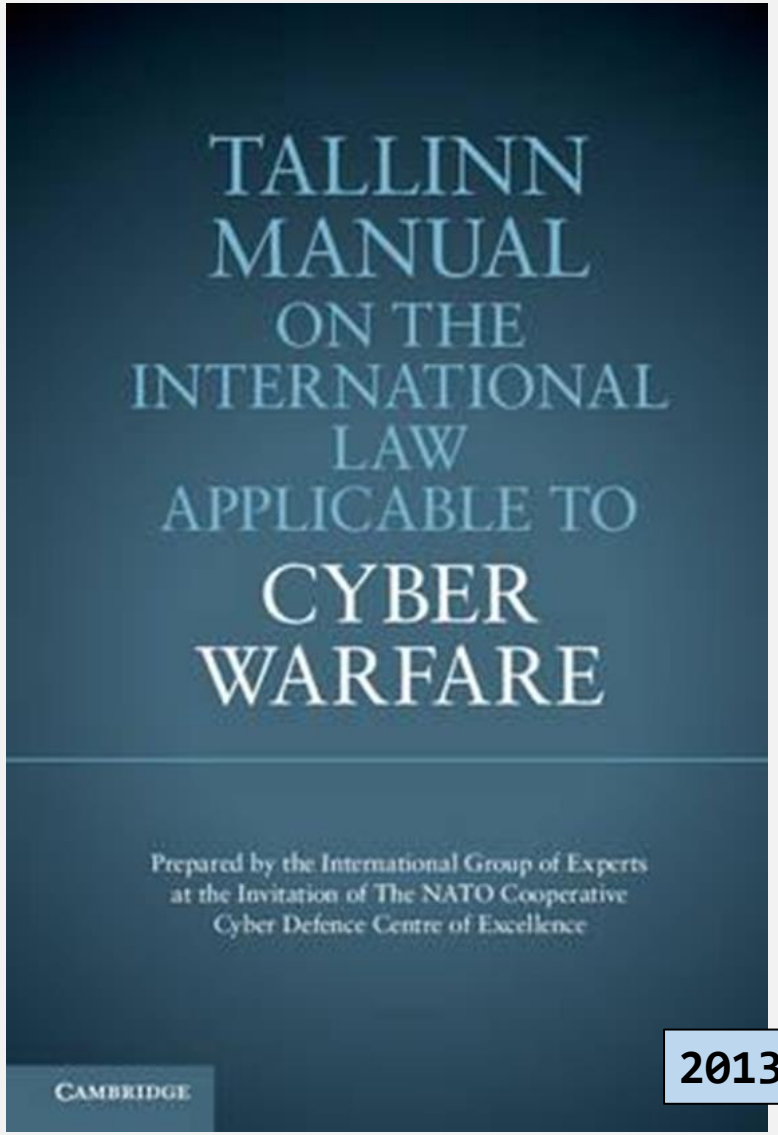
[…] a number of States are developing ICT capabilities for **military purposes**; and that the use of ICTs in **future conflicts** between States is becoming more likely

[…] **international law**, and in particular the Charter of the United Nations **is applicable and essential** to maintaining peace and stability and for promoting an open, secure, stable, accessible and peaceful ICT environment.

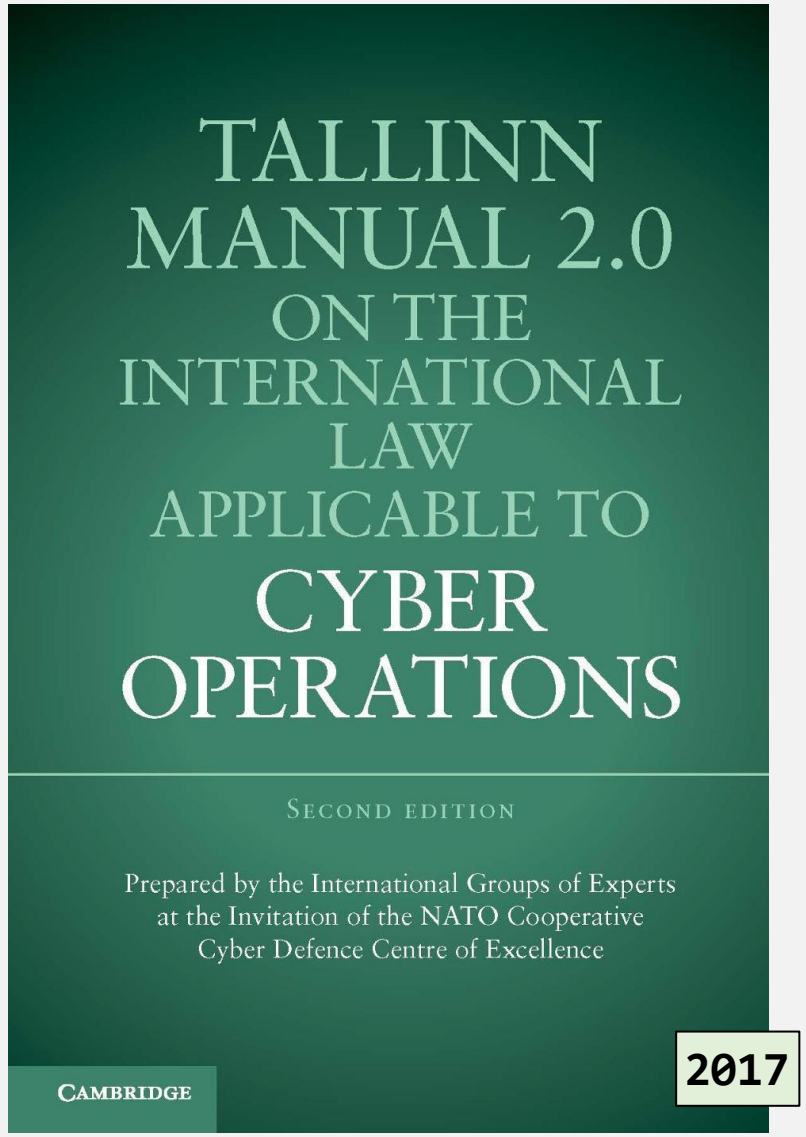
GGE Report: assessments and recommendations of **how international law applies to the use of ICTs** by States

Ciberoperaciones militares: aplicación del Dº Internacional

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia



2013

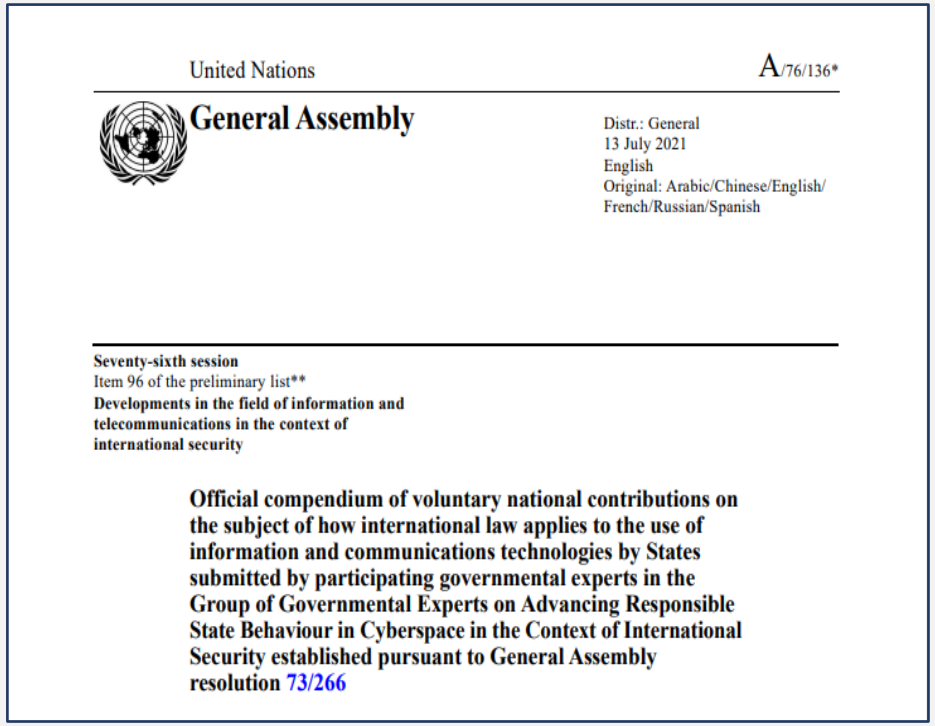


2017

Ciberoperaciones militares: aplicación del Dº Internacional
Posiciones nacionales

Harold H. Koh, Legal Adviser, U.S. Department of State, on September 18, 2012, at the USCYBERCOM at Fort Meade, Maryland.

- Los principios del Derecho Internacional son aplicables al ciberespacio.
- El ciberespacio no es una zona *"law-free"* donde cualquiera pueda realizar actividades hostiles sin reglas o restricciones.



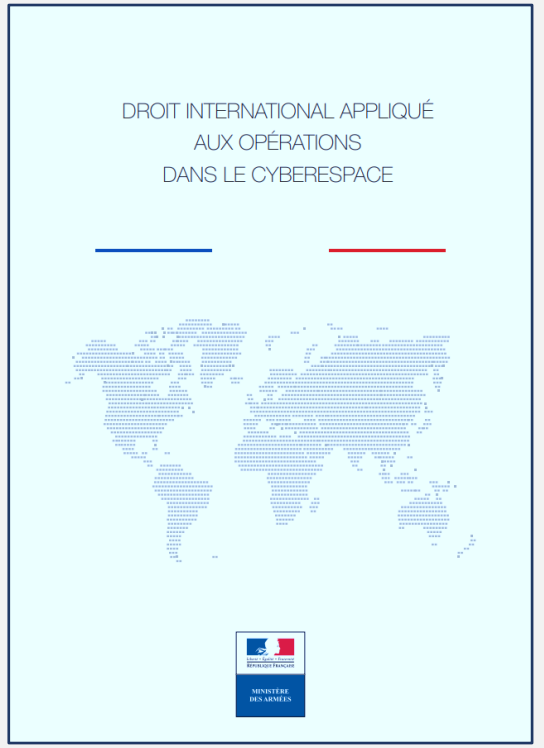
United Nations A/76/136*

General Assembly

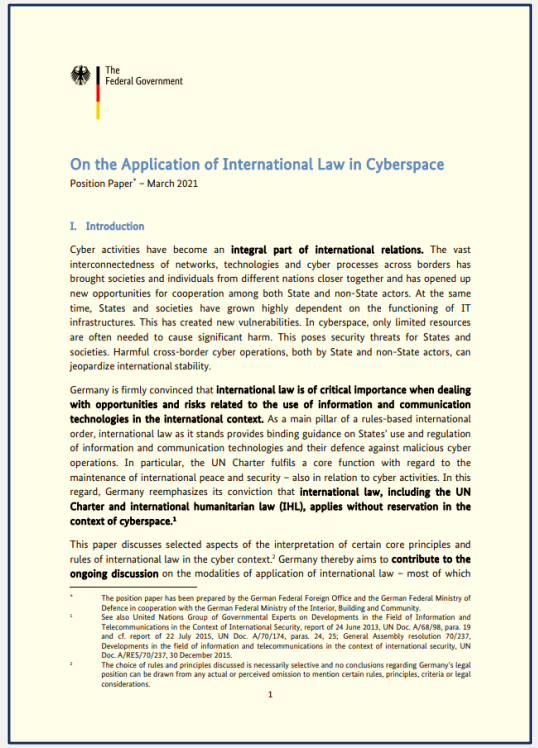
Distr.: General
13 July 2021
English
Original: Arabic/Chinese/English/
French/Russian/Spanish

Seventy-sixth session
Item 96 of the preliminary list**
Developments in the field of information and telecommunications in the context of international security

Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266



DROIT INTERNATIONAL APPLIQUÉ
AUX OPÉRATIONS
DANS LE CYBERESPACE



The Federal Government

On the Application of International Law in Cyberspace

Position Paper* – March 2021

I. Introduction

Cyber activities have become an **integral part of international relations.** The vast interconnectedness of networks, technologies and cyber processes across borders has brought societies and individuals from different nations closer together and has opened up new opportunities for cooperation among both State and non-State actors. At the same time, States and societies have grown highly dependent on the functioning of IT infrastructures. This has created new vulnerabilities. In cyberspace, only limited resources are often needed to cause significant harm. This poses security threats for States and societies. Harmful cross-border cyber operations, both by State and non-State actors, can jeopardize international stability.

Germany is firmly convinced that **international law is of critical importance when dealing with opportunities and risks related to the use of information and communication technologies in the international context.** As a main pillar of a rules-based international order, international law as it stands provides binding guidance on States' use and regulation of information and communication technologies and their defence against malicious cyber operations. In particular, the UN Charter fulfils a core function with regard to the maintenance of international peace and security – also in relation to cyber activities. In this regard, Germany reemphasizes its conviction that **international law, including the UN Charter and international humanitarian law (IHL), applies without reservation in the context of cyberspace.**[1]

This paper discusses selected aspects of the interpretation of certain core principles and rules of international law in the cyber context.[2] Germany thereby aims to **contribute to the ongoing discussion** on the modalities of application of international law – most of which

* The position paper has been prepared by the German Federal Foreign Office and the German Federal Ministry of Defence in cooperation with the German Federal Ministry of the Interior, Building and Community.
1 See also United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, report of 24 June 2013, UN Doc. A/68/98, para. 19 and cf. report of 22 July 2015, UN Doc. A/70/174, paras. 24, 25; General Assembly resolution 70/237, Developments in the field of information and telecommunications in the context of international security, UN Doc. A/RES/70/237, 30 December 2015.
2 The choice of rules and principles discussed is necessarily selective and no conclusions regarding Germany's legal position can be drawn from any actual or perceived omission to mention certain rules, principles, criteria or legal considerations.

1

Ciberoperaciones militares: aplicación del Dº Internacional
Posiciones nacionales

National positions

Edit | Edit Source

- African Union (2024)
- Australia (2020)
- Brazil (2021)
- Canada (2022)
- China (2021)
- Costa Rica (2023)
- Czech Republic (2020 and 2024)
- Denmark (2023)
- Estonia (2019 and 2021)
- Finland (2020)
- France (2019)
- Germany (2021)
- Iran (2020)
- Ireland (2023)
- Israel (2020)
- Italy (2021)
- Japan (2021)
- Kazakhstan (2021)
- Kenya (2021)
- Netherlands (2019)
- New Zealand (2020)
- Norway (2021)
- Pakistan (2023)
- Poland (2022)
- Romania (2021)
- Russia (2021)
- Singapore (2021)
- Sweden (2022)
- Switzerland (2021)
- United Kingdom (2018, 2021 and 2022)
- United States (2012, 2016, 2020 and 2021)

Ciberoperaciones militares: aplicación del Dº Internacional
Posición de España

PDC - 3.20

DOCTRINA DE OPERACIONES EN EL ÁMBITO CIBERESPACIAL

AJP-3.20 "ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS" CON ELEMENTOS NACIONALES ESP

ABRIL - 2021

USO OFICIAL

NATO STANDARD
AJP-3.20

ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS

CON ELEMENTOS NACIONALES DE ESPAÑA

Edition A Version 1

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED ADMINISTRATIVE PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

USO OFICIAL

Chapter 3 – Planning and conduct

Section 1 – General

3.1. All cyberspace operations (COs) are likely to be an integral part of Alliance operations and missions (AOM) and need to be considered from the early stages of planning. Due to the inherent sensitivities of some COs their planning may have to be compartmented. Planning for activities in or through cyberspace should identify areas where these activities could create effects or substitute other means that could create similar effects. Expertise in being able to identify, describe and develop possible effects and decisive conditions in cyberspace should be available to the commander, as well as the ability to identify risks involved with activities in or through cyberspace.

3.2. The commander should, to the maximum extent possible, deconflict, synchronise, and coordinate activities in all domains to obtain the desired effects.

Section 2 – Legal considerations

3.3. NATO Allies recognise that international law applies in cyberspace.[19] NATO COs must be conducted in accordance with international law, including the United Nations (UN) Charter, Law of Armed Conflict (LOAC)[20] and human rights law,[21] as applicable.[22] As a matter of principle, Allies contributing COs on behalf of the Alliance must conduct those COs consistent with applicable international law, as well as adhere to their own relevant national laws.

3.4. The legal framework applicable to and the required authority to conduct COs depends on the nature and context of the activities, such as, but not limited to:

- a North Atlantic Council (NAC) approved operation plan and annexes to include rules of engagement (ROE)[23] for COs, as applicable;
- standing authority or policy;
- the expected effects of COs;

[19] Wales Summit Declaration, 5 September 2014.
[20] Also known by many Allies as International Humanitarian Law.
[21] Warsaw Summit Communique, 8-9 July 2016.
[22] Additionally see AJP-01, *Allied Joint Doctrine*, subsection on *Use of force in international law*, for details on the three basic criteria in international law (self defence, United Nations Security Council mandate, or invitation by host-nation state), under which NATO can act as an international political and military cooperation organisation; all of which apply in the cyberspace domain as they do in the other operational domains. [22] See AJP-01, *Allied Joint Doctrine* for details on ROE.
[23] See AJP-01, *Allied Joint Doctrine* for details on ROE.

Ciberoperaciones militares por debajo del umbral del uso de la fuerza

Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins. **Continuous engagement** imposes tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks.

The Department will campaign in and through cyberspace **below the level of armed conflict** to reinforce **deterrence** and frustrate adversaries.

The Department will campaign in and through cyberspace to generate insights about malicious cyber actors, as well as **defend forward** to disrupt and degrade these actors' capabilities and supporting ecosystems.

Ciberoperaciones militares por debajo del umbral del uso de la fuerza: Soberanía

¿Qué ciberoperaciones constituyen, por sus **efectos**, una violación de la **soberanía territorial**?. Parece claro que lo son las que causan **daños físicos o lesiones**. Sin embargo, los efectos **más probables** de las ciberoperaciones serán la **pérdida (temporal o permanente) de la funcionalidad de los sistemas** cibernéticos o la manipulación o alteración de los datos. La mayoría de los Estados consideraría una **pérdida permanente** de funcionalidad como el **equivalente de un daño físico** a la infraestructura cibernética afectada o a los sistemas que dependen de ella. Por debajo de ese umbral, **falta consenso** sobre la naturaleza o la gravedad de los efectos que permiten calificar la ciberoperación como violación de la soberanía territorial. **Francia**, no obstante, ha manifestado que el mero hecho de **causar efectos** en territorio francés es suficiente para violar su soberanía.

En cuanto a la **interferencia con funciones inherentemente gubernamentales**, la celebración de elecciones y la actividad policial son los ejemplos paradigmáticos, pero la **defensa nacional** también es una función inherentemente gubernamental.

Como se señaló la **Corte Internacional de Justicia** en su sentencia en el caso **"Nicaragua"** (1986), la intervención prohibida requiere de 1º) el uso de **"coerción"**, 2º) que incida en el **"dominio reservado"** del Estado objetivo (un área de actividad que el derecho internacional deja a los Estados). Reducida a lo básico, la intervención implica obligar al Estado objetivo a emprender actividades o tomar decisiones, o abstenerse de ellas, en contra de su voluntad.

Michael N. Schmitt: *"[…] las decisiones y actividades **militares y políticas** serían los objetivos lógicos de las ciberoperaciones […] y cumplirían con el estándar. Así lo haría, por ejemplo, una ciberoperación que interfiriera significativamente con la planificación y ejecución de **despliegues avanzados** de EE.UU. en Europa. También las ciberoperaciones contra la **economía** de un pequeño Estado de la OTAN de tal severidad como para obligarlo de facto a votar de una manera particular en el Consejo del Atlántico Norte. Por el contrario, las ciberoperaciones que simplemente generan un **sentimiento interno** contra la participación de EE.UU. o de otro Estado en los asuntos de seguridad europeos no alcanzarían el nivel de intervención".*

Ciberoperaciones militares equivalentes a un uso de la fuerza

Las ciberoperaciones pueden violar la prohibición de Derecho internacional consuetudinario sobre el **uso de la fuerza**, codificada en el **artículo 2(4) de la Carta de las NU**. Todos los Estados están de acuerdo en que la prohibición se aplica en el contexto cibernético; el desafío radica en identificar aquellas operaciones que cruzan el **umbral** del uso de la fuerza.

Hay acuerdo en que una ciberoperación que cause **daños físicos o lesiones** importantes equivale a un uso de la fuerza, al igual que una operación que cause una **pérdida sustancial en la funcionalidad** del sistema atacado. Por debajo de ese umbral, no hay consenso entre los Estados, aunque, cada vez más, se tiende a adoptar un enfoque caso por caso que evalúa la **"escala y efectos"** de la ciberoperación para determinar si cruza la línea del uso de la fuerza.

Este enfoque atiende a una **variedad de factores** como, entre otros, la gravedad de las consecuencias de la ciberoperación, la situación geopolítica, la trayectoria del Estado autor, la inmediatez con que se manifiestan sus efectos, la entidad que inicia la operación (militar, servicios de inteligencia, por ejemplo) y la naturaleza del objetivo atacado.

Respuestas permisibles: retorsión y contramedidas

Retorsion

Unfriendly but not unlawful

Acto u omisión **inamistoso** pero que **no viola ninguna norma** de Derecho internacional. Por ejemplo, las sanciones económicas impuestas a Rusia en respuesta a su ataque armado contra Ucrania.

Las **contramedidas** son actos u omisiones de un Estado que violarían el derecho internacional de no ser por el hecho son **respuesta a actos u omisiones ilícitos** de otro Estado y tienen por objeto hacer que ese Estado desista y proporcione las reparaciones que pudieran corresponder. Una contramedida no necesita ser de la misma especie que el acto frente al que se responde.

Respuestas permisibles: Acciones realizadas en legítima defensa

Artículo 51 de la Carta de las Naciones Unidas : *"Nada de lo dispuesto en la presente Carta menoscabará el* ***derecho inherente a la legítima defensa individual o colectiva*** *si se produce un* ***ataque armado*** *contra un Miembro de las Naciones Unidas, hasta que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales"*.

La opinión dominante es, en palabras de la Corte Internacional de Justicia en *"Nicaragua"*, la de que un ataque armado es la **"forma más grave"** de uso de la fuerza. Por tanto, la escala y efectos de cualquier ciberoperación tendrían que ser especialmente graves para activar este derecho. Puede ser necesario que se produzcan daños físicos o muertes, si bien **Francia** ha adoptado una visión amplia al sugerir que una ciberoperación sería un ataque armado *"si causara una pérdida sustancial de vidas o daños físicos o* ***económicos considerables****"*.

Ciberoperaciones en conflictos armados: Aplicación del Derecho Internacional Humanitario

CICR

Derecho internacional humanitario y ciberoperaciones durante conflictos armados

Documento de posición del CICR

Dirigido al Grupo de trabajo de composición abierta sobre los Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, y al Grupo de expertos gubernamentales sobre la Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional.

Noviembre de 2019

Índice

Resumen 2
I. Introducción 4
II. El posible costo humano de las ciberoperaciones 4
III. La aplicación del DIH a las ciberoperaciones durante los conflictos armados 5
IV. La protección que otorga el DIH vigente 6
V. La necesidad de debatir cómo se aplica el DIH 8
El uso militar del ciberespacio y los efectos sobre su carácter civil 8
La noción de "ataque" según el DIH y las ciberoperaciones 9
Datos civiles y el concepto de bienes de carácter civil 10
VI. Atribución del comportamiento en el ciberespacio a los efectos de la responsabilización de los Estados 10
VII. Conclusión 11

¿Pueden las ciberoperaciones, por sí solas, **desencadenar** un conflicto armado?

¿Qué ciberoperaciones serían equivalentes a un **"ataque"** en el sentido del DIH (artículo 49 PA I)?

¿Gozan los **"datos civiles"** de la protección que el DIH dispensa a los bienes civiles?

Protección de **ciberinfraestructuras de doble uso**, militar y civil.

Participación directa en las ciberhostilidades. El **"IT Army"** ucraniano.

Aplicación del DIH en el ciberespacio: Cibercrímenes de guerra

HUMAN RIGHTS CENTER
UC Berkeley School of Law

Presentación ante la CPI de **cinco casos** de ciberataques rusos contra infraestructuras civiles en Ucrania, que creen deberían investigarse como posibles crímenes de guerra: ataques a la **red eléctrica de Ucrania** en diciembre de 2015, diciembre de 2016 y abril de 2022. Además, incluye el ataque de malware **NotPetya** en 2017 que causó pérdidas de millones de dólares y afectó a más de 60 países, y el ataque a la red de **módem satelital Viasat** utilizada por el ejército de Ucrania, el día de la invasión, que también afectó a varios países europeos.

Si bien ninguna disposición del Estatuto de Roma está dedicada a los delitos cibernéticos, dicha conducta puede cumplir potencialmente con los elementos de muchos delitos internacionales básicos ya definidos.

Los intentos de afectar a infraestructuras críticas, como instalaciones médicas o sistemas de control para la generación de energía, pueden tener consecuencias inmediatas para muchos, en particular para los más vulnerables. En consecuencia, mi Oficina reunirá y examinará pruebas de esa conducta. Asimismo, somos conscientes del uso indebido de Internet para amplificar el discurso de odio y la desinformación, que pueden facilitar o incluso conducir directamente a la comisión de atrocidades.

PREGUNTAS Y
RESPUESTAS

General Auditor Jerónimo Domínguez Bascoy
Centro Superior de Estudios de la Defensa Nacional
(CESEDEN)
Tel.: 913 482 593
Móvil: 620 034 135
email: jrodbas@fn.mde.es