Assessment of the French and Dutch Perspectives on International Law and Cyber-Operations

Brett van Niekerk, Trishana Ramluckan, Daniel Ventre

Assessment of the French and Dutch Perspectives on International Law and Cyber-Operations

Brett van Niekerk[1], Trishana Ramluckan[1] and Daniel Ventre[2]
[1]University of KwaZulu-Natal, South Africa
[2]CESDIP, CNRS, France
vanniekerkb@ukzn.ac.za
ramluckant@ukzn.ac.za
daniel.ventre@cesdip.fr
DOI: 10.34190/EWS.20.029

Abstract: Cyber-operations have altered the nature of war and the applicability of international law to this new form of conflict has been widely debated; however, no clear consensus in this regard has been reached. Challenges that contribute to the uncertainty of international law's applicability to cyber-operations include the difficulty of attribution of cyber-attacks, and translating state sovereignty into Cyber-space. Academic and advocacy groups have provided publications with proposals for international law and cyber-operations; however, these documents are non-binding. In 2019, both France and the Netherlands released their official perspectives on international law and cyber-operations. This paper compares and assesses these two national documents using the NVivo software to conduct qualitative document analysis. The analysis highlights challenges in applying international law to cyber-operations, and illustrates the similarities and contradictions in the national perspectives as compared to each other and the guidelines set out by previous authoritative documents.

Keywords: Attribution, cyber-law, cyber-operations, international humanitarian law, sovereignty

1. Introduction

Warfare and conflict have evolved through the use of cyber-operations, and there has been a marked increase in possible state-backed operations in cyberspace since the mid-2010's, including allegations of the Ukrainian power grid being affected (Greenberg, 2017), interference in the 2016 US presidential elections (DNI, 2017), reported airstrikes in retaliation for persistent cyber-attacks (Fingas, 2019), and reported cyber-attacks in retaliation for physical attacks (Doffman, 2019). The International Institute for Strategic Studies (2018: 6) states that:

> *Cyber capability should now be seen as a key aspect of some states' coercive power, giving them the chance to wage covert digital campaigns. This might be an adjunct to military power, or employed in its place, in order to accomplish traditional objectives. This has driven some European states to re-examine their industrial, political, social and economic vulnerabilities, influence operations and information warfare, as well as more traditional areas of military power.*

The growing prevalence of cyber-operations in international relations gives rise to the need of assessing the applicability of international law to this new form of conflict. Whilst the relevance of international law to cyber-attacks and cyber-operations has been widely debated, there is yet to be an official agreement on this matter. Examples of challenges include the need for attribution which is difficult in cyber-space, and uncertainty of how concepts such sovereignty and use of force apply in a virtual context. The most in-depth study resulted in two publications that provide guidelines and suggestions for the application of international law in cyber-space: the Tallinn Manual on the International Law Applicable to Cyber Warfare (Schmitt, 2013) and the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Schmitt, 2017). In 2015 a United Nations document examined the impact on growing information technology on national security (United Nations, 2015). In 2019, France and the Netherlands released their official national stance on this matter, International Law Applied to Operations in Cyberspace (Ministère des Armées, 2019) and International Law in Cyberspace (Netherlands Parliament, 2019b), respectively. These are the first national stances that have been published, illustrating foreign perspectives on cyber-operations.

The two national documents have been the subject of numerous readings and comments (in the media, on the Internet, on specialized websites) but academic works are necessary to methodically analyse the postures of the States. This paper aims to: (1) to identify the importance placed on various concepts of international law by the two national documents; (2) to investigate the relationship amongst the various legal aspects; (3) to identify

challenges raised by the international documents, and any measure to mitigate these; and (4) to assess the alignment of the national documents to existing authoritative (but compliance is not mandatory) documents. To achieve these aims, the NVivo software is used to conduct qualitative document analysis.

The paper continues in Section 2, which presents a background to the previous efforts assessing international law and cyber-operations. The methodology is described in Section 3, and the results of the document analysis is presented in Section 4. A summary of the results is provided in Section 5, followed by the conclusion in Section 6.

2. Background

There has been extensive academic and professional debate regarding the application of international law in cyber-space. A primarily academic enquiry soliciting input from a panel of experts produced two outputs, being the two *Tallinn Manuals* referred to in Section 1 (Schmitt, 2013; Schmitt, 2017). These guidelines often indicate the views of the experts, and differences of interpretation or opinions that exist, indicting ongoing uncertainty in how international laws can be translated into a virtual world. In November 2018 the *Paris Call for Trust and Security in Cyberspace* (2018) was released, however this aligns more to the combatting of cyber-crime, but does refer to the Budapest Convention which sets out mechanisms for law enforcement operations in cyber-space that could occur across national boundaries (Council of Europe, 2001). In December 2018, the Global Commission on the Stability of Cyberspace released the *Singapore Norm Package*, which focusses on the responsibilities of states to ensure a safe, secure and available Internet (GCSC, 2018).

These documents and related legal concepts have undergone commentary and further academic discussion. Kilovaty (2014) further investigated the challenges with *Jus ad Bellum* in cyber-space with reference to the first *Tallinn Manual*; Student n°2222171 (2016) considered this in terms of the attempts at regulation and possible humanitarian impact. Eilstrup-Sangiovanni (2018) motivates for a dedicated international convention on cyber-warfare. Lindsay (2015) specifically focusses on attribution and deterrence in cyber-space, and Lotrionte (2012) considers the concept of state sovereignty and self-defence online.

The Netherlands national perspective that is considered is an appendix to a letter dated 5 July 2019, sent to the Netherlands Parliament by their Foreign Minister (Netherlands Parliament, 2019a; Netherlands Parliament, 2019b). The letter and the appendix were in response to requests regarding initiatives to strengthen international law in cyber-space and emerging from an inquiry into espionage attributed to Russia (Netherlands Parliament, 2019a). The Dutch document was published publically on the 26 September 2019, after the French published the document *International Law Applied to Operations in Cyberspace* (*Droit international appliqué aux operations dans le cyberespace*) on the 9 September (Ministère des Armées, 2019; Roguski, 2019). Roguski (2019) considers this document a consolidation of the French perspective exhibited in three documents related to defence and cyber-security from 2013, 2017 and 2018: the *White Book on Defense and National Security* (Livre blanc sur la défense et la sécurité nationale), *International Cyber Strategy* (Stratégie internationale de la France pour le numérique), and the *Strategic Review of Cyberdefense* (Revue stratégique de cyberdéfense), respectively.

3. Methodology

Qualitative document analysis of the two national documents is conducted, in particular content analysis and thematic analysis of the documents using word frequencies, coding, and clustering. The software NVivo was used to conduct the analysis as it provides the functionality to perform all the analytic methods.

For the coding, a total of thirteen codes (also called nodes in NVivo) were used. Two codes are related to the challenges and uncertainty, and a further nine conceptual codes (relating to major themes of international law) were identified from the previous documents, including: armed conflict; attribution; human rights; non-intervention; operations outside of conflict; response/retaliation; responsibility and due diligence; sovereignty; and use of force. A further two conceptual codes (child nodes) were unidentified whilst coding the documents: cyber-weapon, and pre-emptive response. Only content of the documents directly related to the application of international law to cyber-operations was considered; background information and challenges regarding international law in general were excluded from the coding. Clustering and Pearson's Correlation were used to determine relationships amongst the codes, and relationships between the national documents and the previous relevant documents. The previous documents considered include the two Tallinn Manuals (Schmitt,

2013; Schmitt, 2017), the Singapore Norms (GCSC, 2018), and the Paris Call (2018). The latter two documents are considered as they were released within 12 months of the two national documents, therefore will have considered current events. Word frequencies, visualised by word clouds, are used to illustrate major concepts in the various documents and coding. In these instances, common words and obvious words (international, law, cyber) were excluded.

4. Analysis of the National Documents

This section presents the results of the analysis. The section is broken into four sub-sections: Section 4.1 provides a summary of the analysis of the national documents; Section 4.2 focuses on the conceptual codes; Section 4.3 considers the uncertainty and challenges; and Section 4.4 provides an assessment of the alignment between the two national documents and previous authoritative documents.

4.1 Summary of the Analysis of the National Documents

A high-level summary of the two national documents is provided in Table 1. As is evident, the French document is considerably larger (twice that of the Dutch document), which corresponds to the number of text references to the two documents. The percentage coded and the number of codes (nodes coding) are similar for the two documents; the two extra coding nodes in the French document are the two identified during analysis (the pre-emptive response and cyber weapons). The Pearson Correlation between the two documents in terms of word similarity is 0.36, indicating some similarity does exist. It should be noted that the French document has a focus on cyber-operations specifically, whereas the Dutch document has a broader focus on cyber-space, as indicated by their respective titles.

Table 1: Summary of Documents

Document	Pages	Words	Paragraphs	Nodes Coding Source	Coded Percentage	Text References
France	20	11568	323	13	0.2840	157
Netherlands	9	6459	121	11	0.2644	67

Table 2 provides a comparison of the coding per source. Due to the French document being larger, there is a greater degree of coding in that document; however, the coding references and coded words for sovereignty and non-intervention in the Dutch document is greater, and the coding (references and words) is close between the documents for use of force and uncertainty. The two codes unique to the French document are again illustrated. The focus of the French document on cyber-operations and in particular cyber-warfare is evidenced by the coding for armed conflict.

Table 2: Comparison of Coding per Source

	France		Netherlands	
	Coding References	Words Coded	Coding References	Words Coded
Armed conflict	49	3619	4	245
Cyber-weapon	5	292	0	0
Attribution	13	780	9	684
Challenges	7	352	2	38
Human rights	13	994	4	314
Non-intervention	2	100	4	239
Operations outside of conflict	2	86	2	45
Response, retaliation	26	1524	12	1032
Pre-emptive	1	65	0	0
Responsibility and due diligence	12	715	3	228
Sovereignty	11	585	13	638
Uncertainty	3	91	3	92
Use of Force	13	833	12	784

Figure 1 provides a comparison of the word frequencies of the two documents, visualised using word clouds. The prevalence of the words align to the theme of the document titles. The focus on cyber-operations and cyber-

warfare in the French document is evident as the word 'armed' is the most prevalent, with words such as 'military', 'cyberattack', 'conflict' and 'effects' appearing relatively frequently. In comparison, the Dutch document has 'states' as the most frequently occurring word (also prevalent in the French document), with 'sovereignty', 'government', 'human', and 'right(s)' appearing relatively frequently. These words infer the broader application of international law to cyberspace as the title suggests.

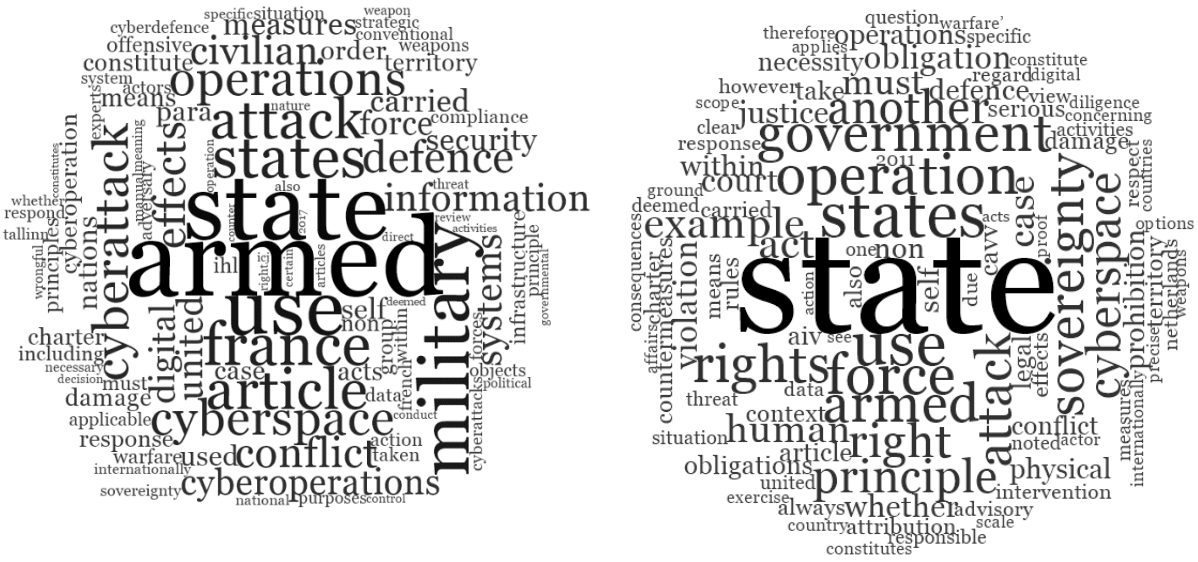

Figure 1: Word Cloud Comparing the French (left) and Dutch (right) Documents

4.2 Conceptual Codes

Table 3 provides a breakdown of the references and coded words per conceptual code for both national documents combined. As can be seen, armed conflict, response/retaliation, use of force, sovereignty, and attribution are the top five (in that order) based on references; however, for the number of coded words human rights exceeds sovereignty. These themes align to major concepts that are currently the focus of debate when applying international law to cyber-space.

Table 3: Summary of Conceptual Codes

Node	Number of Sources	Coding References	Words Coded	Paragraphs Coded
Armed conflict	2	53	3,864	106
Armed conflict\Cyber-weapon	1	5	292	7
Attribution	2	22	1,464	30
Human rights	2	17	1,308	37
Non-intervention	2	6	339	6
Operations outside of conflict	2	4	131	5
Response, retaliation	2	38	2,556	69
Response, retaliation\Pre-emptive	1	1	65	3
Responsibility and due diligence	2	15	943	27
Sovereignty	2	24	1,223	34
Use of Force	2	25	1,617	37

Figure 2 presents the word frequency of the coded content, visualised using a word cloud. The predominate words align to those presented in Figure 1, indicating the coded portions of the document (limited to the content explicitly considering cyber-space) is representative of the documents themselves.

Figure 2: Word Cloud for Conceptual Codes

A cluster diagram based on word similarity, illustrating the similarities of the codes, is presented in Figure 3; both the conceptual codes and the challenges and uncertainty codes are presented in this figure for convenience. There are eight main clusters: (1) pre-emptive response and use of force; (2) uncertainty; (3) attribution, response/retaliation and responsibility and due diligence; (4) non-intervention and sovereignty; (5) operations outside of conflict; (6) challenges; (7) cyber-weapon; and (8) armed conflict and human rights. Clusters (1) to (4) are grouped together, and clusters (5)-(8) are grouped together. Table 4 presents the Pearson Correlations of the conceptual codes. This is formatted as a heat map, where dark green of the strongest correlation and dark red is the weakest. This provides a view of the strength of the various relationships amongst the conceptual codes. There are three pairs with the highest correlation (0.66): armed conflict and human rights; and responsibility and due diligence with both attribution and response/retaliation. This is followed closely by two pairs with a correlation of 0.65: response/retaliation with both attribution and use of force. Other notable correlations include sovereignty with responsibility and due diligence (0.57) and non-intervention (0.53) and armed conflict with response/retaliation (0.54).

Response/retaliation has four correlations greater than 0.5, followed by responsibility and due diligence with three. A correlation of greater than 0.5 implies a strong positive relationship. This indicates these two legal concepts are taking precedence in the discussion. This follows as international law is based on the responsibility of nations, however their legal ability to respond to international incidents needs to be considered with reference to the other concepts considered. Armed conflict, attribution and sovereignty all have two correlations above 0.5; this further illustrates these concepts have some significance.

Figure 3: Codes Clustered based on Word Similarity

Table 4: Correlation of Conceptual Codes

	Armed Conflict	Cyber weapon	Attribution	Human rights	Non-intervention	Operations outside of conflict	Response/retaliation	Pre-emptive	Responsibility and due diligence	Sovereignty	Use of force
Armed Conflict		0.5	0.4	0.66	0.26	0.28	0.54	0.12	0.44	0.3	0.47
Cyber weapon	0.5		0.09	0.3	0.1	0.11	0.15	0.01	0.13	0.13	0.24
Attribution	0.4	0.09		0.12	0.35	0.12	0.65	0.12	0.66	0.42	0.39
Human rights	0.66	0.3	0.12		0.13	0.16	0.22	0.01	0.19	0.16	0.22
Non-intervention	0.26	0.1	0.35	0.13		0.15	0.42	0.1	0.38	0.53	0.48
Operations outside of conflict	0.28	0.11	0.12	0.16	0.15		0.18	0.03	0.06	0.27	0.19
Response/retaliation	0.54	0.15	0.65	0.22	0.42	0.18		0.29	0.66	0.48	0.65
Pre-emptive	0.12	0.01	0.12	0.01	0.1	0.03	0.29		0.16	0.06	0.39
Responsibility and due diligence	0.44	0.13	0.66	0.19	0.38	0.06	0.66	0.16		0.57	0.43
Sovereignty	0.3	0.13	0.42	0.16	0.53	0.27	0.48	0.06	0.57		0.42
Use of force	0.47	0.24	0.39	0.22	0.48	0.19	0.65	0.39	0.43	0.42	

4.3 Challenges and Uncertainty

This section focuses on the codes for challenges and uncertainty, which are summarised in Table 5. These two codes are considered separately to provide specific word frequency analysis on what the areas of uncertainty or challenges. As is evident, both documents raised challenges and areas of uncertainty, however more instances of challenges were indicated.

Table 5: Summary of Challenges and Uncertainty Codes

Node	Number of Sources	Coding References	Words Coded	Paragraphs Coded
Challenges	2	9	390	10
Uncertainty	2	6	183	7

Figure 4 presents the word frequencies of the two codes as a word cloud. As can be seen, cyberspace is predominant; however, words such as “application”, “defined”, “actors”, and “effects” are noticeable. This implies that there are challenges/uncertainty regarding the application of the laws or their definition. In addition, there is uncertainty in determining the actors (i.e. attribution) or the effects of cyber-operations.

Figure 4: Word Cloud for Challenges and Uncertainty Codes

Table 6 presents the correlation amongst the challenges and uncertainty codes and conceptual codes. The strongest correlation is between uncertainty and use of force (0.34), indicating that determining what is considered a use of force is still unclear. A correlation of 0.29 is recorded for uncertainty and non-intervention as well as challenges and armed conflict, again implying problems in defining these concepts. Challenges and uncertainty have a low correlation (0.2), indicating the coding of these two was not identical.

Table 6: Correlation of Challenges and Uncertainty Codes with Conceptual Codes

	Armed Conflict	Cyber weapon	Attribution	Human rights	Non-intervention	Operations outside of conflict	Response/retaliation	Pre-emptive	Responsibility and due diligence	Sovereignty	Use of force	Challenges	Uncertainty
Challenges	0.29	0.20	0.18	0.24	0.12	0.04	0.15	0.02	0.20	0.18	0.15		0.20
Uncertainty	0.24	0.07	0.19	0.11	0.29	0.07	0.23	0.13	0.21	0.16	0.34	0.20	

The Netherlands document (2019: 1) suggests “international debate on ways to clarify the application of international law in cyberspace” to resolve the uncertainty. The document also indicates: “The government endorses the generally accepted position that each case must be examined individually to establish whether the ‘scale and effects’ are such that an operation may be deemed a violation of the prohibition of use of force” (p. 4). This is supported in a similar manner by the French document (Ministère des Armées, 2019: 8): “France reaffirms that a cyberattack may constitute an armed attack within the meaning of Article 51 of the United Nations Charter resulting from the use of physical force, if it is of a scale and severity comparable to those .”

In addition, when considering the uncertainty of the effects of cyber-weapons, that “these risks may be contained by the development of specific cyber weapons whose use is decided according to the desired effects” (Ministère des Armées, 2019: 16).

4.4 Alignment with Other Documents

This section assesses the alignment of the two national documents with previous authoritative documents relating to international law and cyber-space. The clustering of the documents is presented in Figure 5. Three

main clusters can be seen: one contains the two *Tallinn Manual* documents, another contains the two national documents, and the third contains the Paris Call and Singapore Norm Package documents (although these last two can also be considered as separate clusters). The clustering of the two *Tallinn Manual* documents is unsurprising. The clustering of the two national documents shows their consistency.

Figure 5: Sources Clustered based on Word Similarity

To further investigate the relationship of the national documents to the other documents, the Pearson Correlation is provided in Table 5, however limited to the two national documents correlated with the others and themselves (the correlations of the other documents amongst themselves is excluded). The strongest correlations (0.76) is between the Dutch document and the Tallinn Manual 2.0, followed by the French document and the first Tallinn Manual. Two correlations of 0.65 are present: the French document with Tallinn Manual 2.0, and the Dutch document with the first Tallinn Manual. These correlations are not surprising as the French document has a stronger focus on cyber-warfare (as does the first Tallinn Manual), whereas the Dutch document considers broader aspects of international law in cyber-space (and the Tallinn Manual 2.0 focuses on cyber-operations).

Table 5: Correlation of National Documents with Other Previous Documents

	GCSC Singapore Norms	Paris Call	Tallinn Manual	Tallinn Manual 2.0	France	Netherlands
France	0.43	0.37	0.72	0.65		0.36
Netherlands	0.45	0.36	0.65	0.76	0.36	

A comparison of the word frequencies for the national documents and the other documents is provided in Figure 6. There appears to be some consistency between the two sets of documents, and there is also consistency with Figures 1 and 2.

5. Summary of Results

The study has four objectives: (1) to identify the importance placed on various concepts of international law by the two national documents; (2) to investigate the relationship amongst the various legal aspects; (3) to identify challenges raised by the international documents, and any measure to mitigate these; and (4) to assess the alignment of the national documents to existing authoritative documents.

Figure 6: Word Clouds Comparing the National Documents (left) with Previous Legal Texts (right)

From Sections 4.1 and 4.2, the major concepts based on the number of references and coded words are armed conflict, response/retaliation, use of force, sovereignty, attribution, and human rights. These themes are consistent with the major areas of debate regarding cyber-operations and international law. In Section 4.2 it was shown that response/retaliation has the strongest correlations (four), followed by responsibility and due diligence with three. Other terms with strong correlation include armed conflict, use of force, human rights, attribution and sovereignty. This aligns to the codes with the most references, reinforcing the importance of these concepts. This also illustrates the linkages amongst the major concepts and therefore the complexities of cyber-operations and international law.

As illustrated in Section 4.3, the strongest correlations are between uncertainty and use of force, uncertainty and non-intervention, and challenges and armed conflict. This implies that there is ongoing concerns regarding the application of international law to cyber-operations, and the key themes identified above may still be subject to interpretation. Proposed measures to mitigate these areas of uncertainty include further international debate and equating the effects of cyber-attacks to those of physical attacks.

There is strong correlation between the Dutch document and the Tallinn Manual 2.0, as well as the French document and the first Tallinn Manual. In the documents, the Dutch explicitly state that the document follows the advice provided in the Tallinn Manuals, whereas in the French document it is stated that there is deviation from the Tallinn Manuals on some points. Despite this, Schmitt (2019) feels that the French position does align with that of the Tallinn Manuals in some respects, such as the definition of attack. Roguski (2019), however, considers that the French position does deviate in places from the Tallinn Manuals and other views. Regardless, the two Tallinn Manual documents can be considered to have strongly influenced the two national documents.

The limitation of the qualitative document analysis is that it does not give sufficient understanding of political or strategic thinking or intent. Future research can combine the document analysis with additional political science analysis. Future research can provide analysis of the two national documents in relation to a broader set of existing documents and commentary, and additional comparisons with any future national perspectives on the applicability of international law on cyber-space and cyber-operations.

6. Conclusion

The prevalence of cyber-attacks in international relations has resulted in renewed focus on the applicability of international law related to cyber-space and cyber-operations. Two countries, France and the Netherlands, released national perspectives on this matter. This paper assessed the two national documents and identified the major themes that the documents focus on, which is in line with existing academic and international debate. There is correlation amongst a number of concepts, further indicating the importance thereof, whilst illustrating the complexity of the topic. There are still elements of uncertainty highlighted by the documents, however in

order to mitigate this there is an attempt to equate the effects of cyber-operations to physical attacks. There is a call for further international debate to aid in reaching consensus regarding the lack of clarity. The study found that there was a strong influence on the national documents by the two *Tallinn Manuals*, even if the documents stated that they deviate from the views in the manuals. There is scope to expand this research as additional commentary and national perspective become available.

References

Council of Europe. (2001) Convention on Cybercrime, Budapest, European Treaty Series - No. 185.

DNI, United States Director of National Intelligence, (2017) "Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections", 7 January, [online], accessed 12 April 12 2018, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Doffman, Z., (2019) "U.S. Attacks Iran With Cyber Not Missiles -- A Game Changer, Not A Backtrack", *Forbes*, 23 June, [online], accessed 12 July, https://www.forbes.com/sites/zakdoffman/2019/06/23/u-s-attacks-iran-with-cyber-not-missiles-a-game-changer-not-a-backtrack/#3970a285753f

Eilstrup-Sangiovanni, M. (2018) "Why the World Needs an International Cyberwar Convention", *Philosophy & Technology* 31, 379-407.

Fingas, J., (2019) "Israel is the first to respond to a cyberattack with immediate force", *Endgadget*, 5 May, [online], accessed 6 May, https://www.engadget.com/2019/05/05/israel-responds-to-cyberattack-with-airstrike/

Global Commission on the Stability of Cyberspace. (2018) *Norm Package Singapore*, November, [online], accessed 30 January 2019, https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf.

Greenberg, A. (2017) "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired,* 25(7), [online], accessed 18 January 2019, https://www.wired.com/story/russian-hackers-attack-ukraine/.

Kilovaty, I. (2014) "Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare", *American University National Security Law Brief* 5(1), 91-124.

Lindsay, J.R. (2015) "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack", *Journal of Cybersecurity*, 1(1), 2015, 53–67.

Lotrionte, C. (2012) "State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights", Emory International Law Review, 26(2), [online], accessed 16 January 2020, http://law.emory.edu/eilr/content/volume-26/issue-2/symposium%20/state-sovereignty-self-defense-in-cyberspace.html

Ministére des Armées, (2019) *International Law Applied to Operations in Cyberspace*, [online], accessed 18 January, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf

Paris Call for Trust and Security in Cyberspace (2018), 12 November, [online], accessed 18 January 2019, https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433.pdf

Netherlands Parliament, (2019a) Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace.

Netherlands Parliament, (2019b) *Appendix: International law in cyberspace*, 26 September, [online], accessed 8 January 2020, https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf

Roguski, P. (2019) "France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I", *OpinioJuris*, 24 September, [online], accessed 26 September, https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/

Schmitt, M.N. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press.

Schmitt, M.N. (2017) *Tallinn Manual 2.0: On The International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.

Schmitt, M.N. (2019) "France Speaks Out on IHL and Cyber Operations: Part II", *EjilTalk*, 1 October, [online], accessed 16 October, https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-ii/

Student n°2222171 (2016) *The Challenges of Cyber Warfare to the Laws of Armed Conflict: Humanitarian Impact and Regulation Attempts*, Master dissertation, University of Glasgow.

The International Institute for Strategic Studies, (2018) "Editor's Introduction: Western technology edge erodes further," *The Military Balance,* 118(1), pp. 5-6.

United Nations. (2015) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July, [online], accessed 27 January 2020, https://dig.watch/sites/default/files/N1522835.pdf