8 The Principle of Non-Interference and Cyber Operations

Snezana Trifunovska[*]

This article aims briefly to discuss the international legal principle of non-interference in internal affairs. This will be done in the light of the alleged Russian backed cyberattacks by cyber espionage groups meddling in the presidential elections in the US and France in 2016-2017.[1] There have been serious claims by both the US and France that the Russian government interfered in the Presidential elections in the two countries through cyber operations consisting of penetration into the campaign servers and leaking of information.

In the US, the intrusion started in July 2016 when the computer network of the Democratic National Committee was hacked releasing thousands of emails with embarrassing revelations leading to the resignation of the Chair of the Committee.[2] In October 2016, one month before the election, the US government formally accused Russia of cyberattacks against the Democratic Party campaign and warned about the consequences of the attacks.[3] The US Office of the Director of National Intelligence stated that the Russian President Vladimir Putin personally ordered an "influence campaign" to harm chances of the Democratic candidate, Hillary Clinton, and to support the Republican candidate, Donald Trump. The campaign consisted of cyberattacks carried out allegedly by two groups associated with Russian Intelligence, Fancy Bear and Cozy Bear.

Generally, foreign interventions in elections are not rare. During the period from 1946-2000 only the US and Russia were involved in about 117 elections around the globe: the US in 81 and Russia in 36.[4] However, in difference from other cases of intervention, the hacks in the US in 2016 involved not just cyberespionage, but included also a third-party organization (WikiLeaks) which published a massive amount of data of the Democratic Party. This is what in some views made ordinary espionage extraordinary and what "potentially invites more ambitious interventions in American democracy in the

* Dr. S. Trifunovska is Associate Professor at the Law Faculty, Radboud University, The Netherlands.

1 Interventions in elections has in the past frequently occurred. According to some sources, only during the Cold War, 117 elections were intervened upon by the superpowers and 69% of these were US interventions. <https://law.yale.edu/system/files/area/center/isp/documents/hacking_the_election_conference_report_11.01.16.pdf>.

2 <www.mjilonline.org/russian-hacking-and-the-u-s-election-against-international-law/>.

3 <www.reuters.com/article/us-usa-election-cyber-idUSKBN13Y1U7>.

4 <https://en.wikipedia.org/wiki/Foreign_electoral_intervention#cite_note-2>.

future".[5] According to the former CIA Director Michael Hayden the Russian Government

> "pulled off a covert influence campaign during the 2016 US election what was not only probably the most successful in recorded history but the Russia's interference in the presidential campaign represents a fundamentally new sort of intrusion into a modern democracy's inner workings".[6]

France also claimed that similar attacks were carried out on the presidential campaign of Emmanuel Macron. Few hours before the polls opened tens of thousands of internal mails and other, allegedly false documents of Macron were released. French media reported that Macron was targeted by a cyber espionage group which is supposedly linked to the Russian intelligence agency GRU.[7] The campaign was attacked by phishing tricks and attempts to install malware on the campaign site.[8] It is not the first time that Moscow is blamed for interference in French elections. In 1974 the main Soviet security agency, KGB, allegedly launched a covert propaganda campaign to discredit both Presidential candidates, Francois Mitterrand and Valéry Giscard d'Estaing.[9] At that time the right-wing paper *L'Aurore* condemned it as an "'intolerable' insertion into French domestic politics" and as "open intervention in national politics".[10] According to *Politico* this time Moscow was"dusting off the KGB's favored subversive toolbox … but with a technological upgrade for the internet era."[11]

Obviously, the rapid development of information technology and the openness and limitless use of cyberspace have brought about new and increased possibilities to illegally intervene in internal or external affairs of other States. It can be expected that in the future interventions by cyber means will increase causing tension in international relations. Current rules of international law prohibit intervention in internal affairs of other States, however these rules were adopted long before the internet era and were based on classical, kinetic means of possible intrusions. Today, the world is completely different: internet brought not only about connectivity on the global level which was before unimaginable, but on its downside, it also brought new security risks for everyone, including States. One of the increased security risks for States is intrusion into their internal affairs

5 Uri Friedman, "What the DNC Hack Could Mean for Democracy. Suspected foreign interference in an American election might be a taste of what's to come", The Atlantic Daily, 2 August 2016, <https://www.theatlantic.com/international/archive/2016/08/dnc-hack-russia-election/493685/>.

6 Andrew S. Weiss, Wall Street Journal February 17, 2017, <http://carnegieendowment.org/2017/02/17/vladimir-putin-s-political-meddling-revives-old-kgb-tactics-pub-68043>, accessed 21 June 2017.

7 <http://fortune.com/2017/04/24/macron-campaign-france-hackers/>.

8 Idem.

9 *See*, Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-1987, August 1987, US Department of State Publication 9627, Released October 1987.

10 <www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/>.

11 Idem.

through meddling in election processes. That imposes the need to reconsider the rule of non-intervention in the light of new realities, by a special focus on its applicability and scope in the electoral processes.

8.1 The Legal Principle of Non-Intervention in the Era of Cyber Technology

Non-intervention in internal or external affairs of other States is one of the basic principles of international law. It is "a corollary of every State's right to sovereignty, territorial integrity and political independence"[12] and is closely linked to these attributes of States. "To ignore [the] doctrine [of non-intervention] is to undermine international order and to promote violence… ."[13] Swiss philosopher, Emer de Vattel, was the first to note the significance of the principle. In his masterpiece, *The Law of Nations*, published in 1758, he wrote:

> "It is an evident consequence of the liberty and independence of nations, that all have the right to be governed as they think proper, and that no State has the smallest right to interfere in the government of another. Of all the rights that belong to a nation, sovereignty is, doubtless, the most precious, and that which other nations ought the most scrupulously to respect, if they would not do her an injury."[14]

The 1933 Montevideo Convention on Rights and Duties of States included the prohibition of intervention in Article 8. A very brief provision: "No State has the right to intervene in the internal or external affairs of another", summarises the core of the meaning of the rule which until today remained unchanged. The UN Charter does not stipulate such an explicit provision, however, in its Article 2(7) the Charter limits the right of the UN to intervene in matters within the domestic jurisdiction of a member State. This kind of intervention by the UN is only allowed in case the State is subject to enforcement measures under Chapter VII of the Charter. Nevertheless, the prohibition to intervene in affairs of other States applies also to UN member States. The non-intervention rule is implied in the principles of sovereignty of States (Article 2(1)), peaceful settlement of disputes (Article 2(3)) and the prohibition of the use of force (Article 2(4)). These Charter's provisions are seen as a basis for the rule of international law regarding non-inter-

12 Oppenheim's International Law, p. 428. Quoted from the Tallin Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, p. 312.

13 Case concerning Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States*, ICJ Judgment of 27 June 1986, Separate Opinion of Judge Nagendra Singh, para. 209.

14 Emer de Vattel, *Le droit des gens*. Quoted from: Simone Zurbachen, "Vattel's 'Law of Nations' and the Principle of Non-Intervention", *Grotiana* 31 (2010), pp. 69-84, at p. 81.

vention.[15] Apart from these conventional rules, States, international organizations and the International Court of Justice (ICJ) have recognized its customary law status:

> "The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; though examples of trespass against the principle are not infrequent, the Court considers it is part and parcel of customary international law … Between independent States, respect for territorial sovereignty is an essential foundation of international relations."[16]

Apart from that, there are a number of General Assembly documents dealing with the principle of non-intervention. The Declaration on the inadmissibility of intervention in domestic affairs, adopted by Resolution 2131 (XX) of 1965, prohibits direct or indirect intervention in internal affairs of other State and confirms an inalienable right of a State to choose its political, economic, social and cultural system without interference in any form by another State.[17] The famous Declaration on friendly relations and cooperation among States, adopted by resolution 2625 (XXV) in 1970, includes non-intervention as a separate principle with several forms of prohibited acts.[18] The Declaration on the inadmissibility of intervention in internal affairs of states adopted by resolution 36/103 in 1981[19] is also considered important as it contains a range of situations in which intervention can occur, although not all its paragraphs reflect rules of customary international law.[20]

However, the existing international documents do not contain any reference to the prohibition of intervention specifically in relation to cyber operations. As a matter of fact, at this moment there is only one legally binding document, the Budapest Convention on Cybercrime, 2001, which regulates the matters of cybercrime and as such does not involve any issues of public international law. So, an answer to the question of the applicability of non-intervention in relation to cyber operations should be found in the interpretation of the existing rules of international law. This is in line with a view that certain principles and rules which are included in the UN Charter and some other international documents (on human rights- and humanitarian law) are applicable in case of cyber operations as well. This view is broadly accepted. A Group of Governmental Experts

15 Tallin Manual 2.0, op. cit. p. 312 (footnote 760).
16 ICJ *Nicaragua* case, op. cit., para. 202.
17 Declaration on the Inadmissibility of Intervention in Domestic Affairs of States and the Protection of Their Independence and Sovereignty, General Assembly resolution 2131 (XX) adopted at its 1408th plenary session on 21 December 1965.
18 Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, General Assembly resolution 2625 (XXV), adopted at the 25th session of the General Assembly, held on 24 October 1970.
19 General Assembly Resolution A/RES/36/103, adopted on its 91st plenary meeting of 9 December 1981.
20 Tallin Manual 2.0, op. cit. 7, p. 312.

established by the GA Resolution 66/24 of 2011, confirmed that "State sovereignty and international norms and principles that flow from sovereignty [like the non-intervention principle] apply to State conduct of ICT-related activities."[21] Consequently, Rule 66 of the *Tallin Manual 2.0*, prepared by the International Group of Experts and published in 2017, modifies the traditional definition of non-intervention principle only to the extent to include cyber means in the prohibition: "[a] State may not intervene, including by cyber means, in the internal or external affairs of another State."[22] According to the commentary of the Expert Group the definition in Rule 66 covers also situations relating to elections in other countries and prohibits, for example, cyber operations to remotely alter electronic ballots and thereby to manipulate an election.[23] This view of the Expert Group is important for the current discussion, however the *Manual* with its 154 "black letter" rules governing cyber operations is not an official document and does not represent official views either of States or of international organizations and therefore can serve only as a point of reference.

8.2 Conditions under Which a Breach of Non-Intervention by Cyber Means Occurs

According to the existing international documents, the rule of non-intervention can be breached in various manners. It can be breached by direct and indirect intervention; by armed intervention as well as by all other forms of interference or attempted threats in the choice of political, economic, social and cultural system and in the formulation of foreign policy.[24] In principle, any form of direct or indirect intervention, or subversion, is considered to be contrary to the principles on which peaceful international cooperation of States should be built and consequently constitutes a violation of the UN Charter. Also prohibited is an interference in internal affairs, which implies a broader prohibition and refers to acts by States that intrude into sovereign prerogatives of another State, but lacks the requisite of coerciveness to rise to the level of intervention.[25] However, the exact scope of the prohibition is not precisely determined.

> "Apart from the prohibition of the use of force [Article 2 (4) of the UN Charter], it is difficult to be categorical about what is, and what is not, prohibited by the principle. Much may depend upon the context, and on relations between

21 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly document A/68/98 of 24 June 2013, para. 20.
22 Tallin Manual 2.0, op. cit., p. 312.
23 Tallin Manual 2.0., op. cit., p. 313.
24 ICJ *Nicaragua* case, para. 205.
25 Tallin Manual 2.0, op. cit., p. 313.

> the States, the general state of society in the States concerned and their level of political development."[26]

It has been mentioned, for example, that diplomats often interfere in the protection of human rights in the countries where they are accredited. That could be seen as conflicting with their duty of non-interference in internal affairs. However, that seems not to be the case because the right of States and international organizations to criticize human rights situation in other countries, is uncontested.[27] Similarly, the US authorities openly confirmed that they intervened in the affairs of a foreign State "for reasons connected with, for example, the domestic policy of that country, its ideology, the level of its armaments, or the direction of its foreign policy".[28] But, according to the ICJ, "these were statements of international policy, and not an assertion of rules of existing international law".[29] At the same time, there is a variety of situations in which the rule can be considered as violated. The determination of whether or not a breach of the rule took place can be made on the basis of two main criteria or conditions: the act in question must be coercive in nature and it must relate to internal or external affairs of the targeted State.[30] Thus, it is in this framework that the question of election meddling by cyber means should be considered.

In the *Nicaragua* case the ICJ held that "Intervention is wrongful when it uses methods of coercion … The element of coercion … defines, and indeed forms the very essence of prohibited intervention…."[31] Coercion is particularly apparent in case of an intervention which uses force, which can be in a direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.[32] In other words, coercion is "most obvious and easily detectable where a State engages in conduct that violates the territorial integrity of another State" like, for example, in the case of using armed force or in cases of traditional espionage or sending agents into the territory of another State to obtain confidential information.[33] But, important for the discussion on cyber operations is the prevailing view that coercion is not limited only to physical force. The understanding of coercion is much broader and includes any act "designed to deprive another State of its freedom of choice, that is to force that State to act in an involuntary manner or involuntary refrain from acting in a particular way."[34] This

26 Michael Wood, Non-Intervention (Non-Interference in Domestic Affairs), Encyclopedia Princetoniensis, The Princenton Encyclopedia of Self-Determination, on-line <https://pesd.princeton.edu/?q=node/258>.
27 Michael Wood, op. cit.
28 ICJ *Nicaragua* case, para. 207.
29 ICJ *Nicaragua* case, para. 207.
30 Tallin Manual 2.0, op. cit., p. 314.
31 ICJ *Nicaragua* case, para. 205.
32 ICJ *Nicaragua* case, para. 205.
33 Russel Buchan, "Cyber Espionage and International Law", in Nicholas Tsagourias and Russel Buchan (Eds.) Research Handbook in International Law and Cyberspace, Edward Elgar Publishing, 2015, p. 181.
34 Tallin Manual 2.0, op. cit., p. 317.

situation can be caused by various means including cyber means as well, as long as a cyber operation seeks a change of conduct on the part of the targeted State. An example of that would be a State A which launches targeted and disruptive DDoS operations against State B in order to compel it to withdraw its recognition of State C.[35] However, as above pointed out, in addition to that, the coercive effort must be designed to influence the outcome in a matter reserved to a targeted State or to influence its conduct in that matter.[36]

The situation of coercion should be distinguished from persuasion, criticism, public diplomacy and/or propaganda which are directed towards influencing rather than compelling the action of the targeted State.[37] An example of interference would be if a State's Ministry of Foreign Affairs publishes content on social media that is highly critical of another State's internal and external policy. This kind of activity is not coercive in nature and therefore does not constitute prohibited intervention.[38] According to some authors, cyberespionage, i.e the use of computer networks to gain illicit access to confidential information, typically held by a government or other organization,[39] is also not always illegal.

> "Illegal coercion implies massive influence, inducing the affected State to adopt a decision with regard to its policy or practice which it would not entertain as free and sovereign State. It is clear that clandestine information gathering as such will not fulfil such requirements."[40]

Whether or not it will amount to the prohibition of non-intervention depends upon its gravity: acts of cyber espionage that can be regarded as insignificant will not trigger the non-intervention prohibition; they must be sufficiently serious in order to warrant the application of international law.[41] In the view of some other experts this is not necessarily so: it is important in each case to look not only at whether there was a massive influence of illegal access to and gathering of information, but also at its context and consequences in order to be able to conclude whether or not the act constitutes a violation of non-intervention.[42] However, governments are on their part much stricter and consider that any form of cyberespionage violates State sovereignty and therefore it is prohibited. Bra-

35 Tallin Manual 2.0, op. cit., p. 318.
36 Tallin Manual 2.0, op. cit., p. 317.
37 Tallin Manual 2.0, op. cit., p. 318.
38 Tallin Manual 2.0, op. cit., p. 319.
39 <https://en.oxforddictionaries.com/definition/cyberespionage>.
40 Katharina Ziolkowski, Peacetime Cyber Espionage – New Tendencies in Public International Law, 2013. Quoted from in Nicholas Tsagourias and Russel Buchan (Eds.) Research Handbook in International Law and Cyberspace, Edward Elgar Publishing, 2015, p. 186.
41 Russel Buchan, "Cyber Espionage and International Law", in Nicholas Tsagourias and Russel Buchan (Eds.) Research Handbook in International Law and Cyberspace, Edward Elgar Publishing, 2015, p. 186.
42 See Tallin Manual 2.0, op. cit., p. 319.

zil, for example, insisted before the General Assembly that State sovereignty extends to information resident in its cyberspace and that accessing or copying such information is a breach of international law.[43]

Besides, the element of coercion should be accompanied by the intervention's intent to coerce a State in a matter of internal affair. In the *Nicaragua* case the ICJ did not consider it necessary to seek to establish whether the concrete intention of the US to secure a change of governmental policy in Nicaragua went so far as to be equated with an endeavour to overthrow the Nicaraguan government. It was for the Court sufficient to establish that the US by its support of the *contras* "intended … to coerce the Government of Nicaragua in respect of matters in which each State is permitted, by the principle of State sovereignty, to decide freely."[44] The International Group of Experts of the *Tallin Manual* deems that this finding applies to cyber operations by analogy.[45]

Obviously, elections are a purely internal affair of States and any interference in elections in a State without that State's consent is prohibited by Article 2 of the UN Charter and the principles of sovereignty and non-interference. The General Assembly repeated that view in several resolutions. In its resolution 45/151 of 1991 the Assembly affirmed that extraneous activities that attempt to interfere in national electoral processes or intend to sway the results of electoral processes, violate the spirit and the letter of the Charter's principles and of the Declaration on Friendly Relations (UN Res. 2625 (XX). It therefore strongly appealed to all States to abstain from providing, directly or indirectly, any form of overt or covert support for political parties or groups which undermine the electoral process in any country.[46] Similarly, in its resolution 50/172 of 1996, the General Assembly reaffirmed that the principles of national sovereignty and non-interference in the internal affairs of any State should be respected in the holding of elections.[47] Electoral assistance to a member State should be provided by the United Nations only at the request and with the consent of specific sovereign States.[48] Therefore, the Assembly once again strongly appealed to all States to refrain from providing support to any political party or group and from taking any action to undermine the electoral processes.[49]

43 Russel Buchan, op. cit., p. 184.

44 ICJ *Nicaragua* case, para. 241.

45 Tallin Manual, op. cit., p. 322.

46 UN General Assembly resolution on Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in Their Electoral Processes, (A/RES/45/151) adopted at its 69th plenary meeting on 18 December 1990, paras. 3 and 4.

47 UN General Assembly resolution on Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in their Electoral Processes (A/50/172) adopted at its 99th plenary meeting on 22 December 1995, Preamble.

48 UN General Assembly resolution on Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in their Electoral Processes (A/50/172) adopted at its 99th plenary meeting on 22 December 1995, para. 4.

49 Idem., para. 5. Similar paragraphs were adopted in GA resolution A/RES/52/119 of 12 December 1997; A/RES/54/168 of 25 February 2000.

With regard to the hacks in the US there is a widespread opinion that by the intrusion into the emails of the Democratic National Committee and their publication, the originator of the cyber operations wished to discredit the Presidential candidate and to exercise influence on the electorate. That this was the case was also confirmed by the founder of WikiLeaks, Julian Assange, who in an interview on British ITV in June 2016 stated that he hoped that the publication of emails would harm Hillary Clinton's chances to win the presidency.[50] Similarly, it was asserted that the cyber operations in the US were intended to change the outcome of the 2016 election in favour of Donald Trump, or, that they were carried out in retaliation against the US-led sanctions regime against Russia or in response to confrontation in Syria.[51] In their Report released in January 2017 the US intelligence agencies observed that the cyber campaign "initially sought to undermine public faith in the US democratic process, "denigrate" Democratic presidential candidate Hillary Clinton and damage her expected presidency. But in time, Russia 'developed a clear preference for President-elect Trump'".[52]

All these statements are important, but for the determination of the breach of non-intervention during the election in the US, essential are not that much the particular goals as it is the fact that the cyber operations were directed at coercing i.e. exercising influence in a matter belonging to the US' internal affairs, were under its jurisdiction and are part of its sovereignty. Therefore, under the condition that the cyber operations in the US were carried out with support from Russia, it can be freely said that Russia violated the principle of non-intervention. This view is also held by the US government according to which "a Russian cyber-attack conducted to sabotage the democratic election in the United States [violated] international law and international norms as established by the United Nations".[53] The same conclusion can be drawn with regard to the hacks in France.

8.3 The Impact of Cyber Operations on Elections

Foreign interventions in elections have certainly some impact on their outcome. It depends on the strength of the intervening and intervened States, as well as on the means of intervention. Traditionally, foreign States use funds and financial or other types of assistance to support election of one of the parties. During his presidency, the former US President Barack Obama used millions of dollars for control of elections in at least six

50 <https://www.nytimes.com/2016/07/27/us/politics/assange-timed-wikileaks-release-of-democratic-emails-to-harm-hillary-clinton.html>.

51 Hacking the Election Conference, Yale Law School, 20 September 2016 <https://law.yale.edu/system/files/area/center/isp/documents/hacking_the_election_conference_report_11.01.16.pdf>.

52 Intelligence Community Assessment, "Assessing Russian Activities and Intentions in Recent US Elections", 6 January 2017, p. 7.

53 Andrew Fletcher, Vol 38 Michigan Journal of International Law, 29 September 2016, <www.mjilonline.org/russian-hacking-and-the-u-s-election-against-international-law/#_ftn6>.

countries with a varied result.[54] Some studies found that electoral interventions in favour of one side increases on average its vote share by about 3 per cent. That effect is large enough to have potentially changed the results in seven out of fourteen US presidential elections in the post-1960 period.[55] With the use of cyber means and computer technology such an assessment would be difficult to make. According to some assessments, there is a low likelihood that anomalies resulting from hacking a large number of computers in the coming elections may have sweeping effect on the election results.[56]

However, we could see from the interventions in the US and France that in both countries cyber operations had a considerable impact and contributed to a certain extent to the discredit of the Presidential candidates. It is hard to say if in France Macron would get a higher number of votes if his emails were not hacked and put online, but in May 2017 French prosecutors opened an investigation into the validity of anonymous files being posted on internet suggesting that Macron illegally had created a shell company on the Caribbean island of Nevis.[57] Similarly, in the US, the hackers leaked nearly 20,000 emails of the Democratic National Committee which directly affected campaign of Hillary Clinton, brought discredit to her and was certainly one of the reasons for her defeat in the election.

8.4 The Relevance of the Status of Hackers and the Issue of Attribution and Responsibility

As said at the beginning, it is believed that the cyberattacks in the US were carried out by Fancy Bear and Cozy Bear. French media reported that in France, Pown Storm, was responsible for the attacks. These groups are well known to internet security experts as cyberespionage groups sponsored by the Russian intelligence services.

Fancy Bear is one of the oldest cyberespionage groups in the world. It has been called differently, like APT 28 (advanced persistent threat), Pawn Storm, Sofacy Group, Sednit, Tsar Team, etc.[58] According to the US cybersecurity company CrowdStrike, it is associated with GRU, the Russian military intelligence agency and is sponsored by the Russian government. Fancy Bear operates since mid-2000s, and it is claimed that its methods are consistent with the capabilities of nation-state actors. The group allegedly attacks governments, military and security organizations such as NATO and its allies.[59] It has

54 Barak Obama was involved in the elections in: Kenya (as US Senator in 2006), Israel, Libya, Macedonia, Honduras and Egypt. See, Steve Baldvin, "Obama's Meddling in Foreign Elections: Six Examples", 14 June 2017, <https://spectator.org/obamas-meddling-in-foreign-elections-six-examples/>.

55 <https://en.wikipedia.org/wiki/Foreign_electoral_intervention>.

56 Hacking the Election Conference, Yale Law School, 20 September 2016, <https://law.yale.edu/system/files/area/center/isp/documents/hacking_the_election_conference_report_11.01.16.pdf>.

57 <www.marketwatch.com/story/french-prosecutors-probe-suspected-attempt-to-discredit-macron-2017-05-05>.

58 <https://en.wikipedia.org/wiki/Fancy_Bear>.

59 Idem.

carried out attacks on the German Parliament, French TV Station TV5 Monde, NATO, the White House, the OSCE and on the France's presidential candidate, Emmanuel Macron.[60] The group is known to serve the political interests of the Russian Government and the infiltration in the computer systems during the elections was allegedly aimed at helping presidential candidates which are favourable to Russia. The sophisticated methods and technics which Fancy Bear uses in its operations is an indication that it is a State-run program and not a gang or a lone hacker.[61]

Cozy Bear is a cyberespionage group classified as advanced persistent threat ATP 29. It is known under different names, like Office Monkeys, CozyCar, The Dukes, CozyDuke and Grizzly Steppe.[62] It is believed that the group originates from a separate Russian intelligence agency and is associated with the Russian Federal Security Service (FSB). Its targets have been, among others, commercial entities and governmental bodies in Germany, Uzbekistan and South Korea. In the US, it has attacked the State Department and the White House.[63]

In order to establish who is responsible for illegal cyber operations in the US and France it is necessary to determine whether the cyber groups acted on their own or on behalf of the Russian government, in which case the wrongdoing should be attributed to it. Because of increasingly high sophistication of cyberattacks the question of attribution continues to be a problematic point in the question of responsibility for illegal cyber operations. It is in some cases not only difficult but impossible to determine their origin with certainty. That is why, despite the allegation that it was quickly identified that Russia was behind the hacking of Macron's emails, a spokesman for French government security agency ANSSI declined to put a blame on any cyber group.

> "What we can establish is that it's the classic operation procedure of Pawn Storm … however, we will not attribute the attack because we can very easily be manipulated and the attackers could pass themselves off as somebody else."[64]

On the other hand, with regard to the US election the situation is different. On the basis of its investigation the US cybersecurity company CrowdStrike concluded that the hackers which gained access to the computer systems were part of APT 28 (or Fancy Bear). The CrowdStrike also discovered that computers of the Democratic National Committee were infiltrated by APT 29 group. As above mentioned, both groups are associated with

60 <https://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack>.
61 <https://en.wikipedia.org/wiki/Fancy_Bear>.
62 <https://en.wikipedia.org/wiki/Cozy_Bear>.
63 Idem.
64 <http://fortune.com/2017/04/24/macron-campaign-france-hackers/> (accessed on 21 June 2017).

the Russian intelligence. Reportedly, the forensic evidence "connecting [the] intrusions to Russian agencies was very strong compared with other cases".[65] That is why in June 2017 the former Director of the Federal Bureau of Investigation (FBI), James Comey stated in his testimony to the Senate Intelligence Committee that there was no doubt that Russia interfered in the 2016 election. He said: "The Russians interfered in our election during the 2016 cycle. They did it with purpose. They did it with sophistication. They did it with overwhelming technical efforts. And it was an active-measures campaign driven from the top of that government …" and yes, that was a hostile act by the Russian government against the United States.[66]

As above said, the question of whether the cyberespionage groups acted on their own or on behalf of the Russian governmental bodies is of a crucial importance for the issue of responsibility. If the cyberespionage groups acted alone and launched cyberattacks on their own their acts can neither constitute intervention, nor they can violate sovereignty of the State to which the operation is launched.[67] That is so 'because these breaches can be committed only by States' and irrespective of the consequences caused by such operations.[68]

However, if the assertion that these groups acted on behalf of the Russian government is correct, then the question of State responsibility occurs. Rule 17 of the *Tallin Manual* regulates the question of attribution of cyber operations by non-State actors which can be both individuals and groups. There are two situations in which cyber operations conducted by a non-State actor are attributable to a State: (a) when a non-State actor engaged in a cyber operation pursuant to the instructions or under direction or control of the State, or (b) when the State acknowledges and adopts an operation as its own. This Rule is a brief version of what is included in Articles 8 and 11 of the Articles on State Responsibility. Russia has never acknowledged or adopted the cyber operations as its own. It has angrily denied the claim by asserting that it was result of 'unprecedented anti-Russian hysteria'. Therefore, Russia could not be held responsible on that ground. What remains to be considered is whether the hackers acted under its direction or control. In order to give rise to responsibility a State should exercise an effective control over the wrongful acts. In the *Nicaragua* case the ICJ held that, "[f]or the conduct to give rise to legal responsibility … it would in principle have to be proved that [the] State had effective control of … the operations in the course of which alleged violations were committed".[69] However, despite the assertion that ATP 28 group is run by GRU and ATP 29 is linked to FSB, one can only assume that during the elections in the US and France

65 Max Fisher, Why Security Experts Think Russia Was Behind the D.N.C. Breach, The New York Times, 26 July 2016, <https://www.nytimes.com/2016/07/27/world/europe/russia-dnc-hack-emails.html>.

66 Full text: James Comey testimony transcript on Trump and Russia, by Politico Staff, 8 June 2017. <www.politico.com/story/2017/06/08/full-text-james-comey-trump-russia-testimony-239295>.

67 Tallin Manual, op. cit., p. 175.

68 Tallin Manual, op. cit., p. 175.

69 ICJ *Nicaragua* case, para. 115.

Russia exercised effective control over these groups. Proving that with certainty would be problematic and would probably require entering into the internal system of Russia which on its own could be a violation of the principle of non-intervention.

With regard to the question of responsibility it should be noted that, unlike in France, the situation in the US is more complicated also because of the claim that during his election campaign the presidential candidate, Donald Trump, cooperated with the Russians and supported the cyber activities in order to get prevalence in the elections. In a press conference, he openly called Russia "to find the 30,000 emails" of Hillary Clinton.[70] In reaction, Hillary Clinton stated: "We've never had a foreign adversarial power be already involved in our electoral process, (and) we've never had a nominee of one of our major parties urging the Russians to hack more".[71] The connections of President Trump with the Russian government during the period of election, are subject to ongoing investigation by the US bodies, but of importance for this discussion is the question if his involvement has certain consequences for the prohibition of non-intervention. According to Rule 66 of the *Tallin Manual* there is no breach of the principle if a targeted State consents to an act that would otherwise amount to a prohibited intervention. This Rule is comparable to Article 20 of the Articles on State Responsibility. Consent is one of the circumstances precluding wrongfulness. Under "State consent" it should be understood that the consent is given by a governmental body or official acting on behalf of the State. However, while by his alleged ties with Russia Donald Trump might have violated certain national laws, his actions are irrelevant for the rules of international law. This is so because at the time when the alleged contacts took place he had no official position and had no capacity to act on behalf of the US government. Under these circumstances, the rule on the consent precluding responsibility does not apply and Russia could be held responsible for the breach of non-intervention rule.

At the end, one of the remaining questions is which measures could be taken against Russia if it could be determined that it was the culprit. Past practices show that in many cases breaches of non-intervention remain without concrete consequences. In any case, the prohibited intervention like in the cases of the US and France, would not justify a military response. One could consider if countermeasures against Russia could be employed. The existing customary rules on State responsibility provide for such a possibility. Article 22 of the Articles on State Responsibility also includes such a provision on countermeasures. With regard to cyber operations, Rule 20 of the *Tallin Manual* stipulates that countermeasures, whether cyber in nature or not, can be taken, but not in response to a cyber operation conducted by a non-State actor unless the operation is attributable to a State.[72] As such countermeasures are subject to certain limitations, one of them being that the purpose of the countermeasures is to induce that State to comply with its obliga-

70 <www.telegraph.co.uk/news/2016/09/05/clinton-grave-concern-russia-interfering-in-us-elections/>.
71 Idem.
72 Tallin Manual, op. cit., p. 113.

tions.[73] This means that the State employing countermeasures should be sure that the breach is attributable to the State against which it undertakes countermeasures. As pointed out above, this is a difficult aspect when cyber means are engaged in a breach because of the difficulties in attribution of the wrongdoing to a particular State. As already pointed out, cyber operations can be very sophisticated and can be designed to mask the originator. If a State employs countermeasures without having full certainty about the wrongdoings of a State against which the countermeasures are undertaken, it could be in breach of international law incurring responsibility.

The US responded to the alleged breach of non-intervention by Russia on two occasions. In December 2016 President Obama decided to expel 35 Russian intelligence operatives from the United States, imposed sanctions on Russia's two leading intelligence services and penalized four top officers of those services.[74] He said that the US acted after "repeated private and public warnings" and that this was "a necessary and appropriate response to efforts to harm US interests in violations of international norms of behaviour."[75] In July 2017 the US Congress went further in its actions against Russia and decided to sweep sanctions legislation to punish Russia for its meddling in the presidential election but also for its aggression in Ukraine and Syria.[76] On its turn, Russia soon after retaliated by a decision to expel 755 US diplomats from Russia by September 2017 and to seize two diplomatic compounds used by the US. In consequence of these decisions, the relationship between the two States further deteriorated and it is not quite clear in which direction the situation will continue to develop. This only proves how essential is the principle of non-intervention to States and how much is the respect of it important for friendly relations between States. In the future, it can be expected that the development of computer technology will bring about new forms of intrusion in internal affairs and new challenges. To deal with these situations it is important that States are aligned with regard to limits imposed to the use of cyber means and to the scope of their impact on the basic principles of international law.

73 Article 49(1) of the Articles on State Responsibility and Rule 21 of the Tallin Manual.

74 <https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html>.

75 Idem.

76 <https://www.nytimes.com/2017/07/22/us/politics/congress-sanctions-russia.html>.