



I want first to thank the organisers of HackLu for making possible such an event and not being mad against me when I say that conference during the working week is for white old men employed in Infosec.

I'm really happy to be here and I cannot wait to hear all of this amazing talks.

As you have obviously noticed, I speak froglish, and I apologize in advance for that.

I hope that like in many technical talks here, you will have a complete understanding's feeling at the end of this.

I will introduce the European Regulation 2019/796, of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

Swwhoami

2

I suggest that we will get deeper in this question later, after this talk because I truly believe that the most important thing should not be who speak, but

1/ how - clearly or not -

2/ Sometime - about what, but it is not the most important

3/ The proof of concept, reproducible at home by everyone - or maybe not at home if it's a bit sensitive. Reproducible, in the legal field means to give the documentation.

I'm interested by this grey field where techniques used in Infosec and Law meet each others. Just to be complet - I'm not a hacker's lawyer; believe me on that and don't ask.

3

Woman law

« Law » is a polysemic word. Short said, the Law is a tool of conflict resolution based on reasonable arguments and due process, related to a social Frame and historically produced through conflicts.

By conflict, I mean, for example, the strong opposition between peoples who are against abortion and peoples who support freedom of choice for Woman. It shows you how the Law is a state at one point in the history and not an intangible truth.

This ability to change is the reason why it's important to know the Law: you cannot change something you don't know.

I'm not telling you that every change is possible. Usually, the global interest of everyone should conduct to adopte the most efficient rule. But in fact; it's not so simple.

Short said, the Law is a tool. And this tool is in competition whit an other tool, called politic.

\$ top -u europa

- 1815
- 1870
- 1914
- 1939
- 0

4

Law is the tool chosen by the Europeans at the end of the Second World War to avoid the 3rd World War. They concluded the European treaties to place the means of production of weapons under the control of all the involved States, and they have placed the protection of human rights as paramount, with specific jurisdictions able to punish the states for violations.

Maybe it's not perfect, but it works. We - I mean the heart of Europa - we have peace since seventy four Years. Before the second World War, there was the first world war. And before that, the Wars between France and Germany twice in every century.

I tell you that Law is produced by conflicts. For the European Law, the conflict lies most often between the Union, who want more power, and the States members; who are not so happy to give up their prerogative. To ensure the effectiveness of European law, it takes precedence over the Law of the Member States, which are obliged to implement it.

The last evolution allows the European Union to lead a common foreign politic and defense. But the Union is not yet a federal state. It's not achieved.

Sgdb regulation2019/796

5

As any act or regulation of the European Union, this regulation have a legal basis, the Article 215 of Treaty on the Functioning of the European Union (TFUE). In short, this text allows the European Council, aka all heads of all member states of the Union, to adopte the necessary measure, even sanctions, including interrupting economic and financial relations, to be taken against non-europeans states or citizens.

Foreign and Security Policy: CFSP belongs to the external action of the EU and its objectives include the preservation of peace, the consolidation of democracy, the rule of law, human rights and international law.

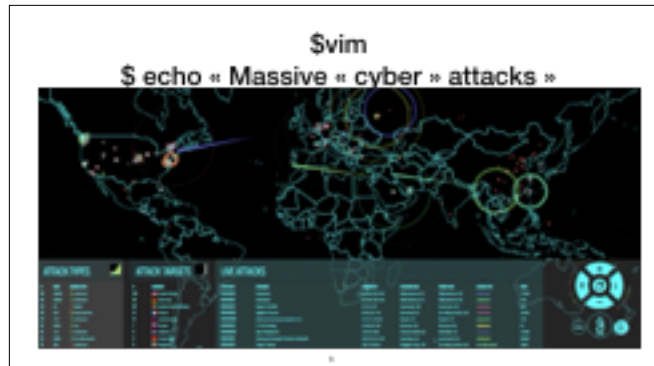
First, it was an implementation of the United Nations (UN) sanctions against states and/or individuals and to fight the terrorism.

But now, it's a tool for the foreign European politic.

It works in two steps: first the Council adopts a decision. This decision is then implemented in Union law (and thus domestically in the EU member states) by virtue of a regulation adopted under TFEU article 215. Our text.

In the past, previous texts have been adopted, as for example (Règlement (UE) n °833/2014 of the 31 juillet 2014 sanctions against high-level Russian and Crimean officials involved in the military occupation of Crimea and responsible for the War against Ukraine. The sanctions include travel bans, asset freezes and a ban on the export of equipment used for war in Ukraine (cf. the work of Kato Verbouwe, source at the end of this presentation).

If I should resume, this Regulation is an old mechanism, which is newly applied to the cybersecurity field, where I'm not sure that it will be really efficient. What says this Regulation?



The article 1 of the Regulation says in his first paragraph: « *This Regulation applies to cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States.* »

The difference between the Directive 2013/40/EU on attacks against information systems his lying in the word « *external threat* ». The Regulation enact the rules concerning the Foreign action of the Union. The Directive concerns the national laws of the members states of the European Union.

The article 1 paragraph 2 describe what kind of Cyber-attacks are an external threat :

- « (a) *originate, or are carried out, from outside the Union;*
- (b) use infrastructure outside the Union;*
- (c) are carried out by any natural or legal person, entity or body established or operating outside the Union; or*
- (d) are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union ».*

The paragraph 3 describe describe what kind of actions are cyber-attack: « *For this purpose, cyber-attacks are actions involving any of the following:*

- (a) access to information systems;*
- (b) information system interference;*
- (c) data interference; or*

(d) data interception,

Not duly allowed.

(where such actions are not duly authorized by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned. »)

You should notice that - private joke in here - there is no definition of « cyber ».

So now, I have a question for you:

Are the massive data interceptions made by the NSA and specially the phone-tapping of Ms MERKEL in the field of the Regulation?

SIs -alth /threat

7

Article 1 paragraph 4 explains: « *Cyber-attacks constituting a threat to Member States include those affecting information systems relating to, inter alia:*

(a) critical infrastructure, including submarine cables and objects launched into outer space, which is essential for the maintenance of vital functions of society, or the health, safety, security, and economic or social well-being of people;

(b) services necessary for the maintenance of essential social and/or economic activities, in particular in the sectors of: energy (electricity, oil and gas); transport (air, rail, water and road); banking; financial market infrastructures; health (healthcare providers, hospitals and private clinics); drinking water supply and distribution; digital infrastructure; and any other sector which is essential to the Member State concerned;

(c) critical State functions, in particular in the areas of defence, governance and the functioning of institutions, including for public elections or the voting process, the functioning of economic and civil infrastructure, internal security, and external relations, including through diplomatic missions;

=> I consider that Merkel's functions are critical State functions.

(d) the storage or processing of classified information; or

(e) government emergency response teams ». So GovCert of every European states members.

And the paragraph 5 : « *Cyber-attacks constituting a threat to the Union include those carried out against its institutions, bodies,*

offices and agencies, its delegations to third countries or to international organisations, its common security and defense policy (CSDP) operations and missions and its special representatives ». And the paragraph 6. *Where deemed necessary to achieve common foreign and security policy (CFSP) objectives in the relevant provisions of Article 21 of the Treaty on European Union, restrictive measures under this Regulation may also be applied in response to cyber-attacks with a significant effect against third States or international organisations.*

This last point is very interesting. It means, for example, that an attack against Ukraine could be in the field of the Regulation.

The paragraph 7 contains term definitions. I will not read that, but you can.

To resume: the Regulation apply to any threat against members states or allies made with cyber attack. It could « soft » cyber attack. I mean social media manipulation, trafficking vote machines, steal of medical data in hospital. And obviously, massive data interception. It can be describe as « soft » because no one is directly killed. But the effects could be giant: influencing on the head of a country, destroying business or reputation of peoples, etc.



This Regulation apply only to massive cyberattack. By massive, it means attack with « *significant effect* ». As this terminology is not really helping, the article 2 of the Regulation try to precise the factors to recognize this « *significant effect* ».

- « (a) *the scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical State functions, public order or public safety;*
- (b) *the number of natural or legal persons, entities or bodies affected;*
- (c) *the number of Member States concerned;*
- (d) *the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property;*
- (e) *the economic benefit gained by the perpetrator, for himself or for others;*
- (f) *the amount or nature of data stolen or the scale of data breaches;*
- or
- (g) *the nature of commercially sensitive data accessed. »*

It means, for example, the phone-tapping of Ms MERKEL because she have critical state function.

But it means too, for exemple, a call to DOSS the Spanish official websites - even if the reason is to promote the independence of Catalonia. We all know that any government will fast use this Regulation against cyber-aktivists and political protestors, if we let them do it.

List



9

The Regulation establishes a framework for targeted restrictive measures.

The first measure is to add the name of the involved person on a **List**, which is published in the full Union. And this is one of the problematic point of this regulation: the decision to add someone on this list is take by the European Council, unanimously.

We know that kind of list in the field of the fight against money laundering and terrorism funding. The list are published and read by any compliance officer of any bank institution. The only thing to notice now is that 6 month after the entry into force of the Regulation the 18 may of this Year, there is nothing on this List.

Who should be reported on this List:

Article 3 paragraph 3 said: Annex I (the list) shall include, (...)

(a) natural or legal persons, entities or bodies who are responsible for cyber-attacks or attempted cyber-attacks;

(b) natural persons or legal persons, entities or bodies that provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission;

(c) natural or legal persons, entities or bodies associated with the natural or legal persons, entities or bodies covered by points (a) and (b) of this paragraph ».

My concern is to understand what means to be « *associated with* ». If I publicly say that Phineas Phisher acted in my opinion for the

good and general interest of anyone, am I to put on this List?
My second concern is that Attribution in the field of Infosec is a real challenge. Even if (I strongly doubt it's possible) some entity could be with 100% certitude being related to a cyber attack, will the politics - the European Council - decide to froze the asset of a country like China or USA?

Measure = fund frizzling

10



If someone will be put on this List, all his fund will be frozen. The article 3 of the Regulation said: « *All funds and economic resources belonging to, owned, held or controlled by any natural or legal person, entity or body listed in Annex I shall be frozen* ». And for being complet, the Council is allowed to refuse access to the European territory to any Person on this List.


As you remember, PayPal froze the account of the Wau Holland Stiftung, the German foundation accepting donations for WikiLeaks when Wikileaks published 250,000 State Department diplomatic cables. Paypal - a privat company - agree to froze the fund whiteout any judicial decision.

As I said before, there is a risk of misuse of this Regulation by governments.

11

Recours

- Don't get caught
- Council
- Court



If your money is frozen, what can you do? Obviously, I cannot help for the first item, and obviously if the fund are frozen, it because you are caught at this time or there is some mistake.

At the beginning of the Regulation, you will find some general ideas about how this rules should be implemented.

« (3) This Regulation respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular the right to an effective remedy and to a fair trial and the right to the protection of personal data. This Regulation should be applied in accordance with those rights ».

The Regulation said in his article 13, Where the Council decides to subject a natural or legal person, entity or body to the restrictive measures, the Council shall communicate the decision referred to in paragraph 1, including the grounds for listing, to the person. This person should have the opportunity to present his observations and / or new evidences. The Council can review his decision. If not, the person can go to the Court.

The Court of Justice of the European Union (CJEU) had expressed in the past that she will review and control any decision take by the Union or a state member on the basis of the article 215 TFUE. It

means too, that any decision based on an acte based on 215 is under the control of the Court.

Rosneft
28 March 2017
Case C-72/15

12

A recent case was about to know if such case, it was possible to request the Court for a preliminary ruling. Judgment of the Court (Grand Chamber) of 28 March 2017 (request for a preliminary ruling) (Case C-72/15)

In short, the Court decide the European rules (that Articles 19, 24 and 40 TEU, Article 275 TFEU, and Article 47 of the Charter of Fundamental Rights of the European Union) must be interpreted as meaning that the Court of Justice of the European Union has jurisdiction to give preliminary rulings, on the validity of an act adopted on the basis of provisions relating to the Common Foreign and Security Policy (CFSP), such as Council Decision 2014/512/CFSP of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, (as amended by Council Decision 2014/872/CFSP of 4 December 2014), provided that the request for a preliminary ruling relates either to the monitoring of that decision's compliance with Article 40 TEU, or to reviewing the legality of restrictive measures against natural or legal persons.

The case: in short, the England ask if it's possible to invest in a company, working in Russia and owned by Russian - Rosneft Oil Company OJSC ('Rosneft').

To resume: if a person is subject to a restrictive measure, directly, she have to presents his observations and evidences to the council. If the Council maintains his decision, then the person can take the case to the European Court.

no liability

13

If there is a mistake and fund get wrongly frozen, what happens?
The Regulation, in his Article 10 express that : « 1. *The freezing of funds and economic resources or the refusal to make funds or economic resources available, carried out in good faith on the basis that such action is in accordance with this Regulation, shall not give rise to liability of any kind on the part of the natural or legal person or entity or body implementing it, or its directors or employees, unless it is proved that the funds and economic resources were frozen or withheld as a result of negligence.*

2. Actions by natural or legal persons, entities or bodies shall not give rise to any liability of any kind on their part if they did not know, and had no reasonable cause to suspect, that their actions would infringe the measures set out in this Regulation ».

Article 11: « 1. *No claims in connection with any contract or transaction the performance of which has been affected, directly or indirectly, in whole or in part, by the measures imposed under this Regulation, including claims for indemnity or any other claim of this type, such as a claim for compensation or a claim under a guarantee, in particular a claim for extension or payment of a bond, guarantee or indemnity, in particular a financial guarantee or financial indemnity, of whatever form, shall be satisfied »*

In short: if your business get destroy because of a wrong decision of the Council in the Attribution of an cyber-attack, it is very sad. But if the restrictive measure is not enforce by a natural person, a company or an institution, this person will be punished. The

régulation express in article 15: « *The penalties provided for shall be effective, proportionate and dissuasive.* »

Conclusion



14

In the Trump case, after months of investigation, the FBI estimate that The Russia interfere whit the US presidential election. Is now the Union cyber-bullet proof? It depends of the decision of the Council: I'm curious to see if the European Union will be challenge the NSA for example.

The Regulation doesn't say anything about the time prescription of action. So I suppose that cyber-attack before the 18the of may are not concerned.

To conclude, I can just say that I'm very curious how in the Future, the European Council and the European Court will handle cyber-attacks cases. I just think it could be a big business field for private investigators because, the person targeted by a restrictive measure have to provide the proof that she is not related to the cyber-attack.

Question(s)?

1lucky1ex@protonmail.ch

@Evematringe

Questions:

- Which interest or relation do have I with the European Union?
- Are this Regulation a legal basis for hacking back?

16

1/ Opinions expressed in this presentation are my own, and do not express the views or opinions of my employer.

I'm a registered lawyer of the Bar of Luxembourg. I'm working for Hance Law SARL, leading by Olivier Hance, esq. I'm not associated in any way to the European Institutions or a company working for the Union.

2/ About hacking back, the best is to review the slides and speaker notes of my talk to Coriin 2016 (<https://www.cecyl.fr/wp-content/uploads/2015/09/CoRIIN2016-04-Eve-MATRINGE.pdf>). Feel free to contact me if you have other question or want to go deeper.

Sources

17

Every materials used to elaborate this talk is here (url).

CAUTION: I don't pretend to be exhaustive.

- <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.ENG&toc=OJ:L:2019:129I:TOC>
- https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp_en
- <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32013L0040>
- <https://www.aclu.org/issues/reproductive-freedom/abortion>
- <https://roguemedia.co/2019/10/18/anonymous-hacker-known-as-xeljomundo-arrested-by-spanish-authorities-faces-11-years/>
- <https://revue-jade.eu/article/download/276/html?inline=1>
- <https://books.google.lu/books?id=yWINDwAAQBAJ&pg=PA1118&lpg=PA1118&dq=TFUE+Article+215&source=bl&ots=d1SErjLRmb&sig=ACfU3U299Ur52aCKA702k2P0iZCovHP8HA&hl=en&sa=X&ved=2ahUKewjqsp-0zKvIAhVoAxAIHcrfC5IQ6AEwBXoECAUQAQ#v=onepage&q=TFUE%20Article%20215&f=false>
- <http://www.gdr-elsj.eu/2012/07/24/cooperation-judiciaire-penale/le-rattachement-de-la-lutte-contre-le-terrorisme-a-la-pesc-ou-comment-la-cour-de-justice-deroule-son-fil-dariane/>
- <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32013L0040>
- https://lib.ugent.be/fulltxt/RUG01/002/163/052/RUG01-002163052_2014_0001_AC.pdf
- https://ec.europa.eu/fpi/what-we-do/sanctions_en
- https://webgate.ec.europa.eu/europeaid/fsd/fsf#!/filesd-list-of-sanctions_en
- <https://www.wired.com/2010/12/paypal-wikileaks/>