**Universidade de Évora - Escola de Ciências Sociais**

Mestrado em Relações Internacionais e Estudos Europeus

Dissertação

# Cibersegurança na União Europeia: A Ciberdiplomacia como ferramenta política de gestão e prevenção de conflitos.

Inês Isabel Baião Serrano

Orientador(es) | Evanthia Balla

Évora 2022

**Universidade de Évora - Escola de Ciências Sociais**

Mestrado em Relações Internacionais e Estudos Europeus

Dissertação

# Cibersegurança na União Europeia: A Ciberdiplomacia como ferramenta política de gestão e prevenção de conflitos.

Inês Isabel Baião Serrano

Orientador(es) | Evanthia Balla

Évora 2022

A dissertação foi objeto de apreciação e discussão pública pelo seguinte júri nomeado pelo Diretor da Escola de Ciências Sociais:

| | | |
|---|---|---|
| Presidente | \| | Irene Viparelli (Universidade de Évora) |
| Vogais | \| | Evanthia Balla (Universidade de Évora) (Orientador)<br>Marco Martins (Universidade de Évora) (Arguente) |

Évora 2022

**Domínio a Investigar/tema:** Cibersegurança na União Europeia

**Questão de pesquisa:** Como a Ciberdiplomacia pode ser uma ferramenta política degestão e prevenção de conflitos na União Europeia?

**Período analisado:** Entre 2000 e 2020.

# Agradecimentos

Primeiramente quero deixar um agradecimento a todos aqueles que fizeram parte do meu percurso académico e que de alguma forma me ajudaram a crescer quer a nível académico quer a nível pessoal e a toda a experiência que me foi proporcionada na Universidade de Évora que terá sempre um lugar muito especial no meu coração.

Não posso deixar de particularizar e dar um agradecimento especial a todos aqueles que fizeram parte desta minha jornada e que me apoiaram:

À minha família, em especial aos meus pais que graças ao seu esforço, apoio e dedicação tornaram este sonho possível, e que sempre me encorajaram a ser melhor e a quem serei eternamente grata;

À equipa de todos os docentes do curso de Relações Internacionais e Estudos Europeus, que com todo o seu profissionalismo e sabedoria me proporcionaram um conjunto de saberes e que me permitiram evoluir a nível académico, também me acompanharam ao longo desta jornada enriquecedora a vários outros níveis.

Em especial à professora Doutora Evanthia Balla, que me deu todo o apoio e ferramentas necessárias à realização desta Dissertação.

Aos meus amigos e colegas de turma e de curso, em especial aqueles com quem criei fortes laços e com os quais espero compartilhar muitos mais momentos daqui para a frente;

A todos aqueles que, de forma direta ou indireta, contribuíram para que fosse possível chegar aqui, nunca me esquecerei dos momentos passados durante estes anos e espero um dia conseguir deixá-los a todos orgulhosos.

# Índice

**Cibersegurança na União Europeia: A Ciberdiplomacia como ferramenta política de gestão e prevenção de conflitos**

# Resumo

Vivemos numa Era na qual a realidade não se limita a barreiras físicas, uma vez que existe um espaço virtual que não conhece limites fronteiriços: o Ciberespaço.

Foram várias as componentes do nosso quotidiano que começaram a intervir nos dois campos acima mencionados, o caso da política, não foi exceção, o que torna necessário a extensão de diversos atores, dentro dos quais a Diplomacia para o Ciberespaço, surgindo assim a Ciberdiplomacia que se torna num ator crucial para dar resposta às questões da comunidade internacional, visando integrar um conjunto de normas e processos que permitam fazer face às ameaças desta Era digital.

Assim sendo, o principal objetivo desta Dissertação de Mestrado passa por compreender como pode a Ciberdiplomacia ser uma ferramenta de gestão e prevenção de conflitos na União Europeia e para tal será aprofundado e analisado o conceito da mesma e os impactos da sua aplicação nos últimos 20 anos.

**Palavras-Chave:** União Europeia, Cibersegurança, Ciberespaço, Ciberdiplomacia, conflitos.

**Cybersecurity in the European Union: Cyberdiplomacy as a conflict management and prevention policy** .

# Abstract

We live in an Era in which reality is not limited to physical barriers, as there are a virtual space that does not know border limits: Cyberspace.

There were several components of our daily life that began to intervene in both fields mentioned above, the case of policy, was no exception, which made it necessary to extension of several actors, within which diplomacy for cyberspace, emerging thus Cyberdiplomacy becomes a crucial actor to answer the questions of international community, aiming to integrate a set of norms and processes that to face the threats of this digital age.

Therefore, the main objective of this Master's Thesis is to understand how can Cyberdiplomacy be a conflict management and prevention tool in European Union and to this end, the concept of it and its impacts will be deepened and analysed.of its application in the last 20 years.

**Keywords**: European Union, Cbersecurity, Cyberspace, Cyberdiplomacy, conflicts.

# Lista de Abreviaturas

CERT'S – Computer Emergency Response Team

CFAA- "Lei Fraude e Abuso de Computador" - Computer Fraud and Abuse Act.

CIA – Central Intelligence Agency- "Agência central de inteligência."

CNCS – Centro Nacional de Cibersegurança

CSIRT – Computer Security Incident Response Team- "Equipa de Resposta a Incidentes de Segurança de Computadores

ENISA - Agência da União Europeia para a Cibersegurança

EUA – Estados Unidos da América.

NATO - Organização do Tratado do Atlântico Norte

NIST - Instituto Nacional de parâmetros e tecnologia dos Estados Unidos.

NSA – Agência de Segurança Nacional

ONU – Organização das Nações Unidas.

PESC- Política Externa e de Segurança Comum da União Europeia

PESD- Política de Defesa e de Segurança Comum

SEAE- Serviço Europeu para a Ação Externa

TIC – Tecnologias de informação e comunicação

UE – União Europeia.

# Introdução

*Apresentação da temática e estrutura da dissertação:*

A natureza global e a alta complexidade do Ciberespaço requerem uma estratégia político-diplomática bem estruturada, onde cada um dos componentes que entram em jogo na Cibersegurança sejam harmonizados, fazendo uso da Ciberdiplomacia. Sabemos que a condução das relações entre estados/países se encontra diretamente ligada com o desenvolvimento da Diplomacia, entendida pelo autor Satow (2012) como sendo a aplicação de inteligência e tino na conduta oficial das relações entre governos independentes ou na conduta de negócios entre os mesmos por meios pacíficos e caraterizada como a arte ou oficio inerente ao desenvolvimento da sociedade, a Diplomacia encontra-se em constante evolução para dar resposta às transformações que ocorrem no mundo quer a nível social, como económico, cultural e político. Desde a sua prática rudimentar até à criação do Estado, a Diplomacia é parte fundamental do desenvolvimento das civilizações e detém um papel fundamental nas Relações Internacionais.

O aparecimento de novos atores internacionais aliado às revoluções tecnológicas e a criação de novas ferramentas e métodos tem proporcionado a necessidade de se adaptar a forma como se praticava a Diplomacia até então a um novo mundo globalizado, onde os problemas globais requerem respostas altamente eficazes e complexas, especialmente a partir do momento em que o virtual se tornou na principal ferramenta da humanidade, e o Ciberespaço numa nova realidade, na qual todos os atores internacionais fazem uso das suas ferramentas para se comunicar e gerar soluções adequadas para fenómenos inter-fronteiras, e os progressos científicos vieram não só revolucionar a incorporação de novos atores no cenário internacional como também dotar a sociedade em geral de uma maior capacidade de desenvolvimento, e tendo em consideração que a sociedade atual é altamente globalizada e o que acontece em determinado local do globo é acessível facilmente em qualquer parte deste através das tecnologias, a Diplomacia até então conhecida necessitou de uma adaptação a este cenário de constantes modificações (Ciberespaço),

originando assim a Ciberdiplomacia, e é precisamente em torno desta, das suas ferramentas e potencial no caso europeu, que se concentra esta pesquisa.

A Ciberdiplomacia por se tratar de um conceito da era digital, acarreta consigo novas perspetivas e dinâmicas relativas ao desenvolvimento das ações por parte dos Estados ou Organizações no cenário internacional, que tem vindo a revolucionar na totalidade a dinâmica das Relações Internacionais e é partindo deste pressuposto que nesta Dissertação de Mestrado é realizada uma análise referente ao quadro de resposta diplomática da União Europeia no âmbito da Cibersegurança, das atividades maliciosas decorrentes no Ciberespaço, dos desafios que dificultam uma resposta unificada por parte dos Estados Membros, bem como as possíveis soluções para fazer face a esses mesmos desafios.

Primeiramente serão conceitualizadas e contextualizadas as definições de alguns termos relevantes para esta Dissertação como "Ciberespaço", "Cibersegurança" e "Ciberdiplomacia", e seguidamente será feito um enquadramento histórico relativamente aos últimos 20 anos, alusivo aos mais recentes incidentes, propostas de cooperação e gestão de conflitos no Ciberespaço que foram decorrendo ao longo do período estudado (2000 a 2020).

No segundo capítulo será introduzida e aprofundada a questão do Soft Power do autor Nye, que consiste numa forma de poder brando no qual a Diplomacia se insere e que se carateriza (muito sumariamente) como a capacidade de uso de atração e persuasão positivas para atingir os objetivos da política externa. É uma ferramenta de poder que não se limita exclusivamente aos Estados, mas que se encontra à mercê de qualquer tipo de ator (estatal ou não-estatal), essencialmente devido ao seu cariz transnacional, indireto e não imediato, sendo um meio "sedutor" que permite atrair e influenciar os seus alvos, sem recurso a qualquer tipo de coação, obrigação ou uso de força, por outras palavras, trata-se de uma articulação branda e sedutora de poder que nos serve como base do enquadramento teórico e que nos ajuda a perceber a sua relação e influência na Diplomacia, mais especificamente na Ciberdiplomacia, uma vez que ambas as terminologias (Diplomacia e Ciberdiplomacia) se constituem como formas de Soft Power.

Posteriormente, será feita uma análise relativamente à situação atual da União Europeia (UE) no âmbito da Cibersegurança, uma vez que centro a minha questão de

pesquisa no caso europeu por se tratar de uma instituição que dispõe de leis comuns a todos os seus Estados Membros e que legisla alguns dos seus assuntos comuns através das suas políticas tais como por exemplo, a PESC, entre outras.

A UE detém um papel fundamental a todos os níveis sobretudo a nível das relações externas e nas questões de defesa e apresenta do ponto de vista internacional diversas missões diplomáticas, (algumas representadas no G8, G20, nas Nações Unidas (ONU), na Organização Mundial do Comércio (OMC), entre outras), e neste âmbito, a Ciberdiplomacia constitui-se como uma ferramenta extremamente poderosa se implementada corretamente e através da cooperação de todos os Estados Membros, pois torna-se necessária a coordenação e cooperação de todos estes países e da UE como um todo para prevenir conflitos no Ciberespaço europeu.

De forma a conseguir dar resposta a todas estas questões, é necessária da parte da UE e respetivos Estados Membros, uma resposta sob a forma de uma politica internacional para o Ciberespaço que valorize os interesses não só políticos mas também económicos e estratégicos da União, sendo para tal, crucial manter as colaborações com os principais parceiros e Organizações Internacionais, e será feito um levantamento de todas as ferramentas de que a UE dispõe nesta área uma vez que a escolha da UE para desenvolvimento desta dissertação, passa também pelo facto da possibilidade desta atuar enquanto "união" e de com a adesão de todos os Estados Membros conseguir mais resultados do que sendo um país "contra o mundo", assim temos uma instituição unida pronta para encarar os desafios internacionais, pois seria uma utopia acreditar que todos os países do mundo se unissem por uma causa como esta, atrevo-me mesmo a dizer que seria impossível, no entanto no que toca ao caso europeu torna-se algo possível e fundamental.

O quarto capítulo estuda o processo evolutivo da Ciberdiplomacia de modo a entender como a Diplomacia se transformou, e analisar quais foram as causas que levaram a essa mudança nos padrões tradicionais de execução da mesma, bem como o impacto desta na esfera internacional e a perspetiva da Diplomacia como ferramenta de gestão e prevenção de conflitos do Ciberespaço no caso europeu (conforme a questão de pesquisa). Este quarto capítulo conceitua todas as noções de Ciberdiplomacia a que nos fornecem as ferramentas necessárias para entender esse processo evolutivo que originou o termo.

A Ciberdiplomacia na UE tem como objetivo desempenhar um papel no cálculo dos potenciais ataques e dos respetivos agressores, atuando como um dissuasor contra o mau comportamento, e embora o conjunto de ferramentas da Ciberdiplomacia seja um complemento das ações de cada Estado Membro, agir em conjunto permitirá que os Estados Membros da União Europeia aumentem a sua credibilidade e sucesso neste ramo, uma vez que respondendo às ciberameaças como ator unificado, a UE terá uma melhor posição na defesa da sua segurança e dos seus interesses políticos e económicos.

Torna-se também evidente que apesar das conversas internacionais sobre Cibersegurança que decorrem na ONU, G20 ou em formatos regionais, vários Estados continuam a realizar ciberataques contra várias entidades da União Europeia.

*Metodologia:*

Relativamente à metodologia usada ao longo desta Dissertação, podemos classificá-la como um ensaio teórico empírico, realizado a partir de uma pesquisa bibliográfica dentro das temáticas de Cibersegurança, o caso especifico da UE e a Ciberdiplomacia, triangulando estas três temáticas com o objetivo de apresentar resposta à questão de partida: Ciberdiplomacia como ferramenta de gestão e prevenção de conflitos na União Europeia.

A estrutura conceitual da tese engloba o Ciberespaço; a Cibersegurança e a Ciberdiplomacia. Igualmente, o conceito liberal de Soft Power de Nye servirá como base argumentativa teórica da presente tese.

Para a recolha de informações relevantes foi realizada uma investigação com base em fontes documentais de índole qualitativa e descritiva.

A literatura académica serviu como fonte principal de dados para esta pesquisa, bem como outros documentos oficiais que forneceram a esta dissertação bastante informação relevante.

Neste sentido foram analisadas diversas obras de autores conceituados bem como artigos académicos, científicos, websites (de instituições governamentais oficiais ou de organismos públicos para recolha de informação estatal disponível online e páginas de

informação de cariz jornalístico), tratados e documentos oficiais.

Também foram tidas em consideração as redes sociais, nomeadamente o Twitter, que permitiu verificar alguns exemplos e informação relevante para a questão de pesquisa.

A pesquisa obtida a partir dessas fontes foi então analisada a fim de determinar o efeito que a Ciberdiplomacia tem nas Relações Internacionais, mais especificamente o seu potencial no âmbito da gestão e prevenção de conflitos na UE, e daí ser tão importante entendermos como funciona a questão da Cibersegurança.

*Relevância e objetivos da Dissertação:*

A escolha da Ciberdiplomacia como figura central desta Dissertação surge pelo fato de considerar que esta poderá ser a solução para procurar alcançar a paz a nível mundial e poderá através da coordenação de esforços fazer face às ciberameaças promovendo um Ciberespaço mais seguro a nível internacional. A minha pesquisa direciona-se para os impactos que a Ciberdiplomacia pode trazer para a União Europeia, quando utilizada como ferramenta integrante do plano estratégico da mesma para a Cibersegurança.

As ações que têm decorrido ao longo dos anos, no ramo da informação e das telecomunicações em contexto de segurança internacional, por parte dos EUA, da UE e da ONU, têm vindo a trazer alertas relativos aos riscos que a revolução digital proporciona, e têm vindo a promover a construção de um novo ambiente de Relações Internacionais, ambiente esse que promova uma cooperação diplomática capaz de conduzir as relações bilaterais e multilaterais do Ciberespaço e respetivo governo, na comunicação internacional e nas políticas globais de informação, tanto os Estados Membros como os seus aliados têm procurado formas de defender a sua soberania e os seus interesses nacionais e globais no Ciberespaço, sejam estes de índole económica, civil ou militar, e este percurso no Ciberespaço tem influenciado decisões a nível político e estratégico, bem como formas de ataque, defesa e dissuasão contra as ameaças que vão surgindo.

Uma vez que toda esta inovação das Tecnologias de Informação e Comunicação, acarreta aconsigo preocupações nomeadamente nas questões de segurança e conflitos,

a Ciberdiplomacia torna-se um ator fulcral para dar resposta às questões da comunidade internacional, visando integrar um conjunto de normas e processos que permitam fazer face às ameaças da Era digital e desta forma torna-se necessário o reforço de uma agenda estratégica internacional que regule a utilização do Ciberespaço, tendo em consideração que um dos grandes desafios do mesmo passa pela dificuldade de atribuição dos ciberataques, uma vez que o uso de sanções tem constituído uma problemática devido às dificuldades na sua definição e aplicação, tendo sido aplicadas no presente ano de 2020, as primeiras sanções contra ciberataques.

A Ciberdiplomacia apresenta-se como um complemento à tradicional Diplomacia, visando promover a segurança do Ciberespaço, e através do desenvolvimento contínuo de respostas diplomáticas a este grande desafio das ciberameaças potencializar o desenvolvimento de novas estratégias que permitam enfrentar os desafios que dificultam uma resposta unificada dos Estados Membros da UE, que minimize os conflitos e compartilhe novos recursos e estratégias entre países, mantendo sempre como base o Direito Internacional, e procurando alcançar a estabilidade global no Ciberespaço.

# 1. Conceptualização e contextualização histórica

Faz sentido que antes de mais nada comecemos por entender um pouco acerca do conceito de Ciberespaço, uma vez que é neste "lugar" que se desenvolve esta dissertação e que é no contexto do mesmo que surgem todos os outros conceitos de prefixo "ciber" analisados adiante, incluindo o termo Ciberdiplomacia de extrema relevância para esta Dissertação uma vez que constitui o foco central da mesma, termo esse que será introduzido neste capítulo e aprofundado nos próximos.

Perceber um pouco da contextualização histórica de todas estas terminologias torna-se fulcral para entender o que conduziu ao seu aparecimento e quais foram os processos cronológicos que vieram trazer significado às mesmas e motivar a urgência do seu aparecimento, de modo a conseguirmos entender a importância não só do Ciberespaço para as Relações Internacionais como também a influência que a Ciberdiplomacia apresenta nesta área, ou seja, importa contextualizar o impacto que o Ciberespaço apresenta na dinâmica das Relações Internacionais, uma vez que é dentro deste que se desenrola toda a ação ciberdiplomática e assim sendo é crucial perceber qual a relação Ciberespaço – Relações Internacionais de forma a perceber como pode atuar a Diplomacia no Ciberespaço (Ciberdiplomacia) no contexto das Relações Internacionais.

## 1.1 Definição de Conceitos

Ciberespaço, é o termo que faz referência ao mundo virtual que surgiu aquando da criação dos sistemas de redes computorizados, é um espaço que apresenta grande impacto nas nossas vidas e que não conhece barreiras físicas, uma vez que todo o desenvolvimento das suas ações ocorre num espaço virtual, (Hermann e Pridohl 2020).

O termo "Ciberespaço" surge em 1982 pelas mãos do autor Gibson através de uma publicação na revista "OMNI", mais tarde, em 1984 o autor usou o termo no seu livro intitulado "Neuromancer".

> *"Ciberespaço. Uma alucinação consensual experimentada diariamente por milhões de operadores em cada nação, por crianças sendo ensinadas através de conceitos matemáticos (...) Uma representação gráfica dos dados dos bancos de cada computador no sistema humano. Inconcebível complexidade"* (Gibson, 1984, pp. 67).

Ou seja, Gibson (1984) terá sido o primeiro a definir o termo Ciberespaço como o ambiente virtual criado pelas redes computorizadas, onde os usuários se conectariam diariamente e interagiriam entre si o que veio originar a expressão "Ciberespaço", associada ao conjunto das informações constantes existentes na internet, e no mundo virtual que ganhou popularidade com o aumento de utilizadores em rede na década de 90, com o aparecimento dos jogos online, das salas de chat e com a possibilidade das mensagens instantâneas todos estes exemplos mencionados com "localização" no Ciberespaço, local que se tornou importantíssimo no inicio do século XXI, para discussões sociais e politicas através de blogs e fóruns de discussão que com a expansão acelerada do Ciberespaço, conduziu ao aparecimento de uma infinidade de possibilidades no mesmo e devido à globalização, o aumento dos desafios com questões relativas à Cibersegurança e às ciberameaças, (Silva, 2009).

Cibersegurança é um termo bastante utilizado, associado aos conceitos de "ciberameaça", "cibercrime" e outros conceitos semelhantes. O termo pode ser utilizado como sinónimo de segurança da informação e dos sistemas (Hermann e Pridohl 2020) e importa fazer referência à definição do Regulamento da Cibersegurança de 2019 (Artigo 2º, n. 1), que diz respeito à perspetiva atual da UE, e que define Cibersegurança como:

> *"todas as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas"*, (Regulamento (UE) 2019/881, 2019, Alínea 1 do artigo 2º).

No entanto, segundo a União Internacional de Telecomunicações – da ONU, o termo (Cibersegurança) surge como sendo um conjunto de ferramentas, estratégias, políticas, normas e diretrizes, gestão de riscos, e todos os elementos que possam ser utilizados para proteger o Ciberespaço e os seus utilizadores.

Da mesma forma que é difícil encontrar um consenso relativamente ao conceito de Cibersegurança, também não é possível estabelecer um conceito comum e fixo para o termo "ciberameaça". No entanto, de acordo com Meulen e Soesanto (2015), existem duas definições que se complementam: Um conceito proposto pela *International Standards Organisation* (ISO) que define ameaça como um potencial evento, que pode causar um incidente indesejado e provocar danos a uma organização ou sistema, e um conceito proposto pelo Instituto Nacional de parâmetros e tecnologia dos Estados Unidos (NIST), que define ciberameaça como qualquer circunstância com potencial de afetar de modo adverso operações ou ativos de organizações ou de indivíduos utilizando como meio um sistema informático cujo acesso seja não autorizado e provocando danos, exposição de dados, alteração de informações ou rejeição de serviços sem autorização.

De modo a garantir a segurança do Ciberespaço, as componentes do nosso quotidiano passaram a intervir não só no "mundo real" mas também no "mundo virtual" (Ciberespaço), o que tornou necessária a extensão de diversos atores estatais e não estatais, dentro dos quais a Diplomacia para o Ciberespaço, surgindo assim o termo "Ciberdiplomacia" que se torna num ator crucial para dar resposta às questões da comunidade internacional.

A Ciberdiplomacia pode ser definida como a Diplomacia no Ciberespaço ou, como o uso de recursos/funções da Diplomacia com o intuito de proteger os interesses nacionais em contexto do Ciberespaço. Segundo Barrinha e Carrapiço (2017) e de acordo com Fletcher (2016), a "Diplomacia virtual" nasceu oficialmente a 4 de fevereiro de 1994, quando Carl Bildt enviou o primeiro e-mail diplomático a Bill Clinton (na altura presidente dos Estados Unidos).

A Diplomacia tem se baseado na crescente dependência da tecnologia para o cumprimento das suas funções daí o termo paralelo Ciberdiplomacia, uma vez que como veremos mais adiante, a Ciberdiplomacia permite a implementação de ações diplomáticas no Ciberespaço fazendo uso das tecnologias para difundir a sua palavra e ações, e de acordo com Potter (2002), o impacto da internet e das novas tecnologias reflete-se nos objetivos, ferramentas e estruturas da Diplomacia. O termo também tem sido usado para descrever a evolução das atividades da Diplomacia pública na era digital e exemplos do uso de TICs

na Diplomacia pública são citados por Potter (2002), que exemplifica rádios, televisões e as novas tecnologias que usam a internet como forma de comunicação, e no caso desta última veremos adiante como por exemplo a utilização das redes sociais por parte dos diplomatas se constitui como uma forma de Diplomacia no Ciberespaço – Ciberdiplomacia.

## 1.1 Contextualização histórica

De forma a conseguirmos dar resposta à questão de pesquisa desta dissertação e percebermos como pode a Ciberdiplomacia ser uma ferramenta eficaz na sua atuação no Ciberespaço é necessária uma contextualização cronológica dos principais acontecimentos históricos marcantes que moldaram o Ciberespaço a um nível internacional.

O termo "ciber", de acordo com Warner (2012), não se trata de um conceito recente e nem propriamente de um conceito do século XXI, e como verificámos anteriormente também não é possível definir a data concreta na qual surgiu o termo "Cibersegurança", no entanto é possível identificar a data em que foi internacionalmente compreendida a necessidade de regulamentar esta vertente "abstrata" da segurança internacional, com a "Lei Fraude e Abuso de Computador" (CFAA), uma iniciativa de organizar o Ciberespaço que consistiu num ato por parte do Congresso dos Estados Unidos (1986) que visava proceder à revisão das leis criminais existentes para crimes cometidos com o auxilio de um computador. Consistiu numa forma de regulamentar a utilização de computadores e este ato converteu-se num exemplo a seguir por todo o mundo, uma vez que foi compreendida a urgência de legislar e regulamentar a utilização de computadores e definir em que consistem e como proceder relativamente às ações levadas a cabo na rede de computadores, o que conduziu a que mais tarde se compreendesse também a necessidade de implementação de uma Diplomacia no Ciberespaço – Ciberdiplomacia, que segundo Fletcher (2016), e conforme referido no capitulo anterior, nasceu oficialmente a 4 de fevereiro de 1994, como verificado anteriormente, através do email enviado por Carl Bildt enviou o primeiro e-mail diplomático ao presidente dos Estados Unidos Bill Clinton, parabenizando-o por levantar o embargo contra o Vietname.

Relativamente às tentativas de regulamentação/legislação do Ciberespaço e de acordo com Warner (2012), foi apenas em 2004 que o primeiro tratado internacional para regular o cibercrime entrou em vigor: A Convenção de Budapeste (A Convenção sobre o Cibercrime), que consistiu num tratado internacional proposto pelo Conselho Europeu com o intuito de identificar os crimes praticados na internet e como atuar nesta perspetiva, e que visava regular a questão da Cibersegurança na arena internacional, já que a história do Ciberespaço tem vindo a lidar com diversos ciberataques que por sua vez contribuíram para que fossem moldados, a estrutura e os recursos atuais da mesma. Segundo Lobato e Kenkel (2015), com o aumento crescente de ciberameaças a nível internacional, tem se observado um aumento crescente da preocupação com as questões de segurança do Ciberespaço, dando lugar a diversos debates por todo o mundo, especialmente após acontecimentos como o ciberconflito entre a Rússia e a Estônia no ano de 2007 e o ciberconflito entre a Rússia e a Geórgia, em 2008 entre tantos outros. Estes acontecimentos são conhecidos mundialmente, uma vez que originaram grandes repercussões na esfera internacional, contribuindo para que a temática da Cibersegurança fosse inserida na Agenda Internacional.

Em 2010, nenhum país ficou indiferente ao aparecimento do vírus Stuxnet que se encontrava a atuar nas instalações nucleares iranianas, com o objetivo principal de provocar danos nas centrífugas do programa nuclear iraniano (Lobato e Kenkel, 2015) e alguns anos depois, entre 2013 e 2015, tem lugar a maior violação de informação da história, através de alguns dos jornais mais importantes dos EUA, informações americanas sensíveis foram tornadas públicas. Snowden, (analista de sistemas conhecido por tornar públicos detalhes privados de vários programas do sistema de vigilância global da NSA americana), comprometendo a segurança de uma das principais grandes potências. Como consequência as preocupações com a vigilância global constante aumentaram e desde este evento, os Estados têm vindo a reforçar os seus esforços na área da Cibersegurança.

Mais recentemente, entre 2017 e 2018, ocorreram outros dois grandes eventos: Wannacry e a violação de segurança do Facebook que tiveram um grande impacto a nível mundial (Fuster e Jasmontaite 2020). Em 2017, o ataque afetou organizações como o Serviço

Nacional de Saúde do Reino Unido, uma companhia telefónica na Espanha, a FedEx e a Deustche Bahn na Alemanha.

O choque internacional foi causado pelo malware conhecido como "WannaCry", software que bloqueia o computador (não pode ser usado até que algum tipo de resgate seja pago), criptografa o arquivo e exige uma espécie de resgate em bitcoins.

Em 2018, foram divulgados dados privados da rede social Facebook de acordo com Miller (2020), os dados de milhões de utilizadores da rede social foram divulgados para fins políticos e influência de eleições e como é óbvio, eventos como os referidos têm conduzido a esfera internacional à preocupação com a Cibersegurança e a necessidade que se coloca de desenvolver estratégias e infraestruturas adequadas para promover uma Cibersegurança eficaz, com o propósito de evitar futuros ataques. Neste sentido, muitos países têm-se mobilizado para encontrar soluções, através de politicas, medidas, estratégias, abordagens bilaterais ou multilateraise legislações que protejam as nações e os utilizadores do Ciberespaço e repensando a importância da Ciberdiplomacia no âmbito da prevenção.

No caso Europeu, e de acordo com Riordan (2019), tanto os governos como os diplomatas têm demorado a aplicar a Diplomacia aos problemas que surgem no Ciberespaço. A Dinamarca foi um dos países pioneiros nessa área uma vez que criou a figura de um "técnico-diplomático" para aprofundar e abordar a realidade do Ciberespaço, (Riordan, 2019), por sua vez na UE, o primeiro documento político abrangente nesta área foi a Estratégia de Cibersegurança da Comissão Europeia e do Alto Representante para 2013, o documento cobriu os ângulos de mercado interno, justiça e assuntos internos e política externa do Ciberespaço.

As linhas principais desta estratégia, defendem a liberdade e abertura da internet, aplicação de regras do mundo físico ao mundo digital, e o fomento da cooperação internacional entre Estados e atores não estatais para prevenir possíveis ameaças.

Atualmente (2020) com a situação pandémica que vivemos, o COVID-19, os níveis de cibercriminalidade têm aumentado em grande escala um pouco por todo o mundo.

> *"(...) este novo ambiente à escala global aumentou a dependência das infraestruturas digitais e os eventuais riscos da sua falha, proporcionando*

> *a exploração do medo e incerteza dos cidadãos por criminosos e suscitar eventuais comportamentos desviantes pela maior presença online."* (Carreiras, 2020, p. 6).

De acordo com o Centro Nacional de Cibersegurança (CNCS) (2020), toda a situação proporcionada pelo Covid-19 teve impacto no aumento das atividades ilícitas online, sendo que o CNCS (2020), afirma existirem pelo menos duas causas plausíveis que passam pelo confinamento social e pela aceleração na adoção das TIC , o que conduziu a uma onda de migração para o mundo online incluindo cibercriminosos e o aumento da utilização do Ciberespaço o que conduziu a um incentivo no sentido de oportunidade dos agentes de ameaças.

Esta breve contextualização, permite-nos perceber que os acontecimentos aqui referidos são apenas alguns exemplos daquilo que moldou de certa forma o Ciberespaço durante os últimos anos, não apenas na UE mas no mundo, e todos os acontecimentos aqui referidos contribuíram de alguma forma para perceber o seu funcionamento, estruturar medidas de Cibersegurança por todo o mundo, acompanhar a relação do Ciberespaço e das Relações Internacionais e para se iniciarem os primeiros passos na questão da Ciberdiplomacia.

## 1.2 Impacto do Ciberespaço nas Relações Internacionais e a influência da Ciberdiplomacia

A internet tornou-se numa ferramenta essencial para o quotidiano do ser humano, uma vez que dependemos diariamente dessa ferramenta e que a utilizamos no nosso dia a dia para as mais vastas funções. É praticamente indiscutível a mudança que esta ferramenta veio trazer à vida de milhões de cidadãos pelo mundo fora, no entanto, analisar como esta inserção do meio digital transformou as relações internacionais já se trata de um assunto mais complexo.

Conforme verificado no capitulo anterior, o Ciberespaço encontra-se intimamente ligado às Relações Internacionais, deixando a sua marca nas mesmas, uma vez que as ações desenvolvidas no Ciberespaço apresentam um impacto direto quer na sociedade como na cultura, na economia, na politica entre outros campos que constituem a comunidade

internacional, logo tornando-se abrangente e suscitando desafios teóricos e práticos no campo das Relações Internacionais (Kremer e Muller, 2013), deste modo, importa contextualizar o impacto que o Ciberespaço apresenta na dinâmica das Relações Internacionais, uma vez que é dentro deste que se desenrola toda a ação ciberdiplomática (foco deste trabalho) e assim sendo é crucial perceber qual a relação entre o Ciberespaço e as Relações Internacionais de forma a perceber como pode atuar a Ciberdiplomacia no Ciberespaço no contexto das Relações Internacionais.

No mundo em constante mudança e evolução no qual vivemos a inexistência do Ciberespaço torna-se inimaginável, no entanto no inicio do século XXI os principais atores internacionais mostraram algumas dificuldades relativamente ao acompanhamento do ritmo dos acontecimentos provenientes das revoluções das TIC e da própria internet ao redor do mundo (Hamdouni, 2013), já que a tecnologia se tornou um fator de poder nas Relações Internacionais desde a revolução industrial, e nos últimos 10 anos, período no qual os avanços tecnológicos conduziram a diversas mudanças a nível internacional como a revolução árabe ou a eleição de Barack Obama em 2008, o que alcançou um grande impacto social, uma vez que estas ferramentas facilitam em grande escala a construção de movimentos de forma rápida e de baixo custo.

Acontecimentos marcantes como o atentado do 11 de setembro de 2001 ou a grande crise económica mundial (2008) vieram agravar o clima de incerteza nas Relações Internacionais, contudo,a Primavera Árabe permitiu averiguar tudo aquilo que havia sido feito até então o que significou um momento fulcral para a sociedade internacional (Hamdouni, 2013), as redes sociais foram cruciais em acontecimentos contra a ditadura nos países árabes, e a Primavera Árabe não teria tido o alcance que teve sem o auxilio destas novas tecnologias, onde foram canalizadas todas as criticas e movimentos contra o abuso de poder.

Outro bom exemplo da amplitude da tecnologia nas Relações Internacionais são as chamadas “smart city’s” (Jimenes, Koutitas e MCclellan, 2018) espalhadas ao redor do mundo, termo que se encontra associado ao desenvolvimento tecnológico integrado numa área urbana. Numa smart city, algumas das funções e serviços próprios da cidade são geridos através de sistemas computadorizados interconectados, desde serviços de saúde a sistemas de transportes e de segurança são alguns exemplos de serviços que se tonam melhorados e mais acessíveis ao estarem conectados a uma rede computadorizada, uma

vez que a recolha de dados se torna numa tarefa muito mais rápida e prática, o que aumenta a eficiência dos serviços prestados. De acordo com os autores Jimenes, Koutitas e MCclellan (2018), os problemas que surgem nos sistemas, ainda que estes sejam seguros, relacionam-se sobretudo com a evolução das tecnologias, isto é, conforme vão aumentando as tecnologias vão aumentando as possibilidades não só boas como maliciosas também e a partir do momento em que uma cidade se conecta ao Ciberespaço, ela pode abrir uma porta relativamente perigosa, especialmente se existir alguma falha de segurança ou um ataque intencionando e isto constitui apenas um dos exemplos de como os serviços governamentais e de utilidade pública assim como a sociedade em geral se encontram interligados nesta rede global, facilitando ações e potencializando interações sem fronteiras nem limites.

Segundo Hamdouni, (2013), a internet conquistou o seu espaço na agenda internacional de debate público e sendo esta uma questão central abrangente a toda a comunidade internacional, rapidamente demonstrou a sua capacidade de influência no âmbito das Relações Internacionais, as TIC e a Internet são hoje o par perfeito e essencial no progresso e na evolução técnica equalitativa das Relações Internacionais, por exemplo, anteriormente os Estados estavam sujeitos à longa espera para receber respostas ou alternativas às suas questões no panorama internacional, o que formulava obstáculos reais ao avanço dos processos no campo da Diplomacia e das Relações Internacionais, atualmente, problemas dessa índole deixam de existir, uma vez que com a implementação dos avanços das tecnologias essesprocessos passam a ser coordenados automaticamente, o que significa um grande avançoem termos de tempo e dinheiro para processamento de informações em frações de segundos e além disso, o envio e a entrega de documentos importantes que outrora eram atrasados por procedimentos complexos, contrariamente ao que sucede hoje em dia, graças à utilização das TIC, com apenas um "clique" é possível enviar e partilhar uma grande variedade de dados para qualquer parte do mundo. Assim, a presença da internet e do Ciberespaço temoferecido um respaldo técnico à Diplomacia contemporânea e à própria Ciberdiplomacia, uma vez que sem a sua presença, não seria possível agilizar todos estes processos complexos da atualidade (López, 2020).

O Ciberespaço, as revoluções das TIC e a globalização vieram reformular o campo da informação que sofreu grandes modificações a nível de desenvolvimento das

comunicações interpessoais, hoje a sociedade não se limita a um diálogo direto entre as pessoas nem a um espaço físico, aliás, se antigamente as pessoas praticamente só se relacionavam pessoalmente, diretamente e num mesmo espaço físico, hoje é possível fazê-lo através de um ecrã sem qualquer limite espacial, como afirmam López (2020), tudo derivado do desenvolvimento das TIC e dos equipamentos de comunicação que transformaram o mundo numa "aldeia global", o que tem vindo a possibilitar que milhões de cidadãos estejam conectados e interajam no Ciberespaço, local no qual convergem muitos dos seus interesses globais o que de certa forma veio modificar as Relações Internacionais, como eram conhecidas até então pois a influência e participação crescente da sociedade civil no âmbito da Relações Internacionais tem fortalecido o monopólio dos Estados relativamente ao papel destes no panorama internacional, uma vez que o Ciberespaço abriu as portas do círculo privado onde os únicos capazes de tomar decisões e executar a Diplomacia eram os atores estatais e, portanto outros atores internacionais foram deixados de fora da política e alguns dos impactos do desenvolvimento das novas tecnologias e da existência do Ciberespaço na política internacional são observados ao longo das décadas, (Riordan, 2019), como é possível verificar nos exemplos a baixo:

Arrais (2014) exemplifica que em 1989, o governo chinês realizou um massacre contra os seus cidadãos em Pequim, foi dito que o evento não teria sido exposto internacionalmente se os estudantes que se encontravam no local não tivessem registado o ocorrido através dos seus telemóveis, câmaras de vídeo e redes informatizadas que permitiram partilhar informações a ativistas de todo o mundo. Desta forma, o governo chinês ficou exposto às críticas internacionais pelos seus atos desumanos.

A Guerra do Golfo constitui outro exemplo no ano de 1991, onde os canais de comunicação foram bloqueados por ordens do Pentágono e tudo era tratado com base num código secreto. Durante este processo, as utilizações de determinadas redes de computadores facilitaram a transmissão de relatórios de informações detalhadas sobre os efeitos da Guerra do Golfo nos países do Terceiro Mundo, bem como em Israel e nos países árabes, afetados principalmente pela proximidade do evento (Arrais, 2014).

De acordo com Hamdouni (2013), foram diversos os acontecimentos marcantes que evidenciaram a existência de um cenário "ciber", porém foi graças à Primavera Árabe que ficou delimitada uma nova era na qual o Ciberespaço mostrou todo o seu esplendor, um

acontecimento que mobilizou multidões de tal maneira nunca antes vista pela humanidade. A comunidade internacional moveu-se em torno de uma única causa, permitindo derrubar os regimes totalitários na Tunísia e no Egito, tudo graças à internet.

Atualmente e tendo em consideração que todos conseguem aceder a um mundo de informações compartilhadas por milhões de utilizadores através do Ciberespaço, os Estados perderam parte do seu poder de imposição, ou seja, torna-se difícil cometer atos violentos ou violar os direitos dos cidadãos sem ficar exposto a milhões de pessoas, por exemplo, o caso WikiLeaks, que segundo Ludlow (2010) veio divulgar uma série de documentos sensíveis de interesse público onde foram expostas atitudes pouco éticas de governos norte-americanos e europeus provocou grande agitação na sociedade internacional, perturbando os principais centros de inteligência europeus e americanos e este é só um dos muitos exemplos que podemos utilizar para afirmar que a internet trouxe à comunidade internacional inúmeros benefícios e enormes mudanças a nível social, económico e politico nas últimas décadas, que vieram modificar quaisquer previsões ou pressupostos teóricos relativos ao Ciberespaço e à influência deste no plano internacional e assistimos cada vez mais na arena internacional, a novas formas de ciberameaças cada vez mais emergentes e em posição no Ciberespaço, o que promove a deslocação do campo de batalha para o mundo virtual.

A internet é uma realidade das Relações Internacionais (Arrais, 2014), já não é possível pensarmos a nossa vida sem ela, não só as novas tecnologias moldaram o mundo como abriram portaspara a questão da segurança. Privacidade e garantias de segurança pelo mundo tornam- se problemáticas atuais, uma vez que é impossível afirmar que um sistema não terá nenhuma falha ou que é totalmente seguro e invulnerável a ciberameças/ataques ou roubode dados.

As Relações Internacionais foram influenciadas por essas grandes mudanças paralelas à crescente participação da sociedade civil no Ciberespaço, alterando parâmetros e cálculos estabelecidos por estudiosos do cenário internacional e onde a informação tem repensado o papel do Estado neste novo espaço de interação global que não conhece fronteiras nem limites físicos e é assim que a dimensão virtual supera a dimensão humana e social, tendo em consideração que perante esta nova realidade, circulam valores em prol de uma sociedade mais aberta e mais democrática que tende a transformar-se numa verdadeira

ideologia que tem vindo a revolucionar formas de pensar e agir nesta nova sociedade virtual, no entanto, é importante referir que existem várias ferramentas no Ciberespaço à disposição das Relações Internacionais e que demonstram grande eficiência, e a Ciberdiplomacia constitui uma delas (Barrinha e Renard, 2017), como veremos, uma vez que é uma poderosa ferramenta com grande potencial, o que neste sentido torna fundamental entender o funcionamento do Ciberespaço, uma vez que este constitui o espaço no qual se realiza esta pesquisa, e que é graças à sua existência que a Ciberdiplomacia ganhou forma e motivo de ser, de igual forma é essencial perceber qual é a relação e o impacto deste no âmbito das Relações Internacionais, para que possamos perceber o impacto que a Ciberdiplomacia apresenta não só no Ciberespaço mas também a sua influência nas Relações Internacionais no contexto do mesmo (Ciberespaço).

A Ciberdiplomacia nada mais é do que o uso de ferramentas diplomáticas no Ciberespaço (Barrinha e Renard, 2017), com o intuito de conduzir as Relações Internacionais, diria até que funciona como um elo de ligação Ciberespaço-Relações Internacionais, já que a Ciberdiplomacia promove uma visão mais aberta, confiável, e segura da informação através do uso da palavra e de meios pacíficos (Soft Power) e que visa fortalecer as infraestruturas de tecnologia, informação e comunicação de modo a fortalecer a paz internacional, a cooperação e as relações amistosas entre países no Ciberespaço, local que constitui um dos maiores desafios da atualidade e que se encontra fortemente vinculado à esfera das Relações Internacionais.

# 2. Enquadramento Teórico

Focando-nos agora no caso específico da Diplomacia no Ciberespaço é importante enquadrarmos as suas origens de forma teórica e desta forma ao longo deste capítulo é introduzida e aprofundada a questão do Soft Power de Nye, que consiste numa forma de poder brando no qual a Diplomacia se insere e que se carateriza (muito sumariamente) como a capacidade de uso de atração e persuasão positivas para atingir os objetivos da política externa. É uma ferramenta de poder que não se limita exclusivamente aos Estados, mas que se encontra à mercê de qualquer tipo de ator (estatal ou não-estatal), essencialmente devido ao seu cariz transnacional, indireto e não imediato, sendo um meio "sedutor" que permite atrair e influenciar os seus alvos, sem recurso a qualquer tipo de coação, obrigação ou uso de força, por outras palavras, trata-se de uma articulação branda e sedutora de poder que nos serve como base do enquadramento teórico e que nos ajuda a perceber a sua relação e influência na Diplomacia, mais especificamente na Ciberdiplomacia, uma vez que ambas as terminologias (Diplomacia e Ciberdiplomacia) se constituem como formas de "soft-power".

## 2.1 Soft Power

Uma vez que esta pesquisa se encontra direcionada para a questão da Ciberdiplomacia, torna-se fundamental compreender as suas origens, pois à medida que os países trabalham para entender o contexto em rápida e constante mudança no qual nos encontramos e procuram ajustar as suas estratégias a estes, os recursos de Soft Power que se encontram ao dispor dos estados compõe a caixa de ferramentas de política externa necessária não só para o presente mas também para o futuro, e neste âmbito sabemos que o poder nas Relações Internacionais tem sido tradicionalmente definido e avaliado em termos "duros" ou segundo Nye (2008), Hard Power facilmente quantificáveis, muitas vezes entendido no contexto do poder militar e económico.

O termo Hard Power (Nye, 2008) é implantado na forma de coerção: uso da força, ameaça de força, sanções económicas ou incentivos de pagamento, no entanto e em contraste com a natureza coercitiva do Hard Power, o termo Soft Power descreve a utilização da atração/persuasão positivas de modo a atingir os objetivos da política externa.

O Soft Power, evita as ferramentas tradicionais de política externa procurando obter influência através da construção de redes, comunicando por meio de narrativas convincentes, estabelecendo regras internacionais e aproveitando os recursos que tornam um país naturalmente atraente para o mundo.

> *"Soft Power is the ability to affect others to obtain the outcomes one wants through attraction rather than coercion or payment. A country's Soft Power rests on its resources of culture, values, and policies."* (Nye, 2008, p.1).

Ou seja, a ideia principal do Soft Power parte da intenção de dar primazia ao poder da influência e da negociação pacifica e não ao uso da força, procurando influenciar indiretamente através de um determinado ator, os comportamentos ou interesses de outros atores/entidades.

O termo Soft Power surge em 1990, no livro de Nye: "Book Bound to Lead that challenged the then conventional view of the decline of American power", e é nos apresentado como uma ferramenta de poder que não se limita exclusivamente aos Estados, mas que se encontra à mercê de qualquer tipo de ator (estatal ou não-estatal), essencialmente devido ao seu cariz transnacional, indireto e não imediato.

Segundo Nye (1990), o termo tem a sua índole baseada em conceitos ideais e culturais,tais como paz, democracia, liberdade, autonomia, igualdade, prosperidade, sustentabilidade, desenvolvimento, entre outros conceitos positivos a nível global e que pertencem à esfera envolvente do próprio conceito (Soft Power). Importante ressaltar o cariz ideológico, social e cultural do Soft Power, Nye (1990) e Azpíroz (2015) destacam que o mesmo deve ser um meio "sedutor" que permita atrair e influenciar os seus alvos, sem recurso a qualquer tipo de coação, obrigação ou uso de força, por outras palavras, trata-se de uma articulação branda e sedutora de poder, que influencia uma pessoa a querer agir da mesma forma que o seu influenciador em vez de a obrigar a agir em conformidade com o mesmo, para tal, a abrangência dos meios de sedução deve ser inclusiva a todas as pessoas sem quaisquer tipos de restrição, caso contrário poderia entrar em conflito com questões democráticas.

Fatores como a liberdade e prosperidade, são entendidos facilmente como formas de Soft Power, uma vez que bem aplicados se tornam valores desejáveis e até vistos como

"metas" para outros Estados e atores, que influenciados por esse exemplo poderão querer segui-lo também de forma voluntária (Azpíroz 2015).

Os países adeptos do uso do Soft Power para facilitar a colaboração positiva estarão em melhor posição para enfrentar a atual incerteza e instabilidade geopolítica e, em última instância, moldar os eventos globais, uma vez que à medida que os governos lutam com um cenário político internacional volátil e procuram ajustar as suas estratégias de política externa em conformidade, é necessário que reavaliem a sua abordagem atual para gerar e alavancar o Soft Power sendo que numa primeira instância deverão ser estabelecidos com clareza os recursos de que os países já dispõe nesta área.

O Soft Power dá a estados menores que nunca seriam capazes de usar a coerção para afetar o comportamento de outros a oportunidade de atrair outros atores para emular a sua posição e inspirá-los a tomar uma ação coletiva (Nye, 1990).

No entanto, não podemos deixar de analisar o termo mais recente Sharp Power, que surgiu no relatório do National Endowment for Democracy de 2017 como forma de contrastar com o Soft Power de NYE, e que argumenta que precisamos repensar o Soft Power, porque:

> *"o vocabulário conceitual usado desde o fim da Guerra Fria não parece mais adequado à situação contemporânea"* (Ludwig e Walker , 2017, p. 7).

descrevem as novas influências autoritárias que se fazem atualmente sentir no mundo como Sharp Power, e de acordo com os autores, é necessário uma adaptação de vocabulário para este fenómeno, pois o que até então entendemos como um Soft Power mais autoritário se define como Sharp Power que consiste numa forma de poder brando um pouco mais ríspido (Ludwig e Walker, 2017). Se por um lado o Soft Power aproveita o fascínio da cultura e dos valores para aumentar a força de um país, o Sharp Power ajuda os regimes autoritários a obrigar o comportamento em causa e a manipular a opinião no exterior. Atrever-me-ia até mesmo a dizer que o Sharp Power é o balanço entre o Soft Power e o Hard Power.

Soft Power, que como verificámos se traduz na capacidade de afetar os outros por atração e persuasão que contrasta com o Hard Power (uso da força e de meios mais ríspidos), muitas vezes é usado para descrever qualquer exercício de poder que não envolva o uso da força.

Nye (2018) por sua vez afirma que se usarmos o termo Sharp Power como abreviatura de guerra de informação, o contraste com Soft Power fica claro. Sharp Power é um tipo de Hard Power. Manipula a informação, que é intangível, mas a intangibilidade não é a característica distintiva do Soft Power. As ameaças verbais, por exemplo, são intangíveis e coercitivas.

Podemos então concluir que existem diversas formas de exercer o poder, no entanto a que mais se adequa a esta pesquisa é o Soft Power, uma vez que é este "poder brando" que engloba a Diplomacia que é o foco desta pesquisa.

## 2.2 Soft Power e Diplomacia

A Diplomacia, como mencionado acima, é essencialmente um instrumento de política externa com o objetivo de desenvolver relações pacíficas entre governos, Estados, países, entre outros atores.

Acontece também que parte desse processo envolve a persuasão, que Nye (2008) mostra como uma componente essencial do Soft Power, ou seja, a capacidade de influenciar o público estrangeiro para aceitar ou aprovar a agenda de política externa do país em questão, e esta persuasão não se limita a construir relacionamentos baseados no ganho ou pressão material, pois existe um importante elemento emocional subjacente às estratégias diplomáticas de sucesso, uma vez que essas ações facilitam relações duradouras entre os países, pois os seus respetivos públicos internos promovem maior cooperação e participação, a chave aqui é a ligação entre Diplomacia persuasiva e a política de identidade: os países usam a Diplomacia pública não apenas para convencer outros de uma agenda política específica, mas também para convencê-los de que as identidades associadas a essas políticas têm valor moral, o que deve ser reconhecido nos seus relacionamentos com os outros.

Se a Diplomacia é o elo entre identidade e emoção, a Ciberdiplomacia também o é. A revolução dos mídia aumentou muito a dimensão e o alcance das estratégias de Diplomacia, e esta digitalização dos mídia significa que legisladores e diplomatas agora enfrentam níveis muito mais elevados de transparência e responsabilidade em todos os seus atos, em parte devido às crescentes expectativas de abertura ao público, tanto interna

quanto externamente. Aliás, a própria Diplomacia é entendida como uma forma de Soft Power, uma vez que a sua origem assenta na base da negociação pacifica (Pamment, 2016).

Segundo Lachs (1962), a Diplomacia nada mais é do que uma habilidade capaz de gerar acordos seja qual for a sua índole, tendo como base o reconhecimento de interesses mútuos, defende que a Diplomacia se trata da negociação pacífica (Soft Power) como meio para as partes em conflito poderem estabelecer a ordem e soluções para os seus problemas comuns.

Para Nye (2008) falar de Diplomacia é abordar a relação existente entre duas ou mais entidades ou sujeitos de Direito Internacional que possuem direitos e obrigações impostos pela legislação internacional. Os Estados são regra geral, os principais intervenientes das Relações Internacionais e são encarregues pelo ordenamento internacional imposto por uma série de regras inter-estatais estabelecidas através de acordos de cariz jurídico, que servem para regular as relações inter-estatais e entre intervenientes da comunidade internacional, por sua vez, segundo o autor Nicholson (1996), a Diplomacia é um elemento chave necessário e fundamental para qualquer tipo de relação entre os intervenientes e nações, e é uma forma de negociação que tem acompanhado o percurso da história desde os seus primórdios, que se foi consolidando e conceptualizando.

De modo a melhor compreender a Diplomacia na prática (o que nos permite perceber as bases da Ciberdiplomacia) importa ressaltar a convenção de Viena (1961), na qual foi traçado o perfil da Diplomacia, uma vez que foram delineados os elementos chave que a caraterizam:

> *"As funções de uma Missão diplomática consistem, entre outras, em:*
>
> *a) representar o Estado acreditante perante o Estado acreditado;*
>
> *b) proteger no Estado acreditado os interesses do Estado acreditante e dos seus nacionais, dentro dos limites permitidos pelo direito internacional;*
>
> *c) negociar com o Governo do Estado acreditado;*
>
> *d) inteirar-se por todos os meios lícitos das condições existentes e da*

*evolução dos acontecimentos no Estado acreditado e informar a esse respeito o Governo do Estado acreditante;*

*e) promover relações amistosas e desenvolver as relações econômicas, culturais e científicas entre o Estado acreditante e o Estado acreditado.*

*2. Nenhuma disposição da presente Convenção poderá serinterpretada como impedindo o exercício de funções consulares pela Missão diplomática.* " (Convenção de Viena, 1961, artigo 3º).

Com base na citação acima, é possível identificar os pontos chave que caraterizam a Diplomacia, sendo que em primeiro lugar é nos apresentado um sistema de intervenientes que interagem e estabelecem relações de igualdade entre si e em seguida a negociação como processo através do qual serão conduzidas pacificamente as relações entre os intervenientes, o que por sua vez conduz a uma relação direta e imediata entre ambos, e posteriormente, dependendo como corra a negociação será documentado o progresso feito até ao momento final da discussão.

A finalidade da Diplomacia passa por contribuir com uma relação pacifica que irá manter um sistema ordenado através da intensificação das relações amistosas e da paz entre os intervenientes internacionais, e uma vez que como referido anteriormente Soft Power foi cunhado por Nye (1991) como uma ferramenta pacifica e positiva e que a Diplomacia como verificado possui capacidades que podem criar situações e entendimentos comuns para alcançar objetivos internacionais, podemos facilmente classificar a Diplomacia como um recurso de Soft Power e vice-versa .

> *"Soft Power resources often work indirectly by shaping the environment for policy, and sometimes take years to produce desired outcomes"* (Nye, 2004, p. 99).

Isto é, o Soft Power nada mais é do que a habilidade de influenciar e moldar as preferências de terceiros, não é propriedade exclusiva de nenhum país por exemplo, acontece com empresas, atores não governamentais, organizações, entre outros. Na política internacional, o Soft Power de determinada nação assenta basicamente nos recursos culturais, nos valores políticos e nas politicas externas.

O Soft Power é omnipresente a todos os níveis do comportamento humano, de indivíduos a nações, e provavelmente tornar-se-á cada vez mais importante devido à revolução da informação na qual vivemos.

Se o Soft Power pode ser entendido como uma forma de atração, e se por sua vez, a Diplomacia detém os métodos e as ferramentas que permitem fazer uso dessa forma de atração, é possível que os Estados possam aumentar a sua influência sobre outros mediante o seu nível de atratividade, sempre com o propósito de que tal atração permita ao seu Estado atingir os seus objetivos. Ou seja, Soft Power é uma das ferramentas de poder das quais a Diplomacia, sob o ponto de vista de estratégia influenciadora e pacifica dispõe, (Nye, 2008).

## 2.3 "Ciber" Soft Power

Como verificado anteriormente, se a Diplomacia e o Soft Power se complementam mutuamente, e se a Diplomacia atuar no Ciberespaço (Ciberdiplomacia), tratar-se-á de uma extensão do Soft Power a este domínio (Ciberespaço), tornando possível a existência de um "Ciber – Soft Power", isto é um Soft Power a atuar no Ciberespaço (CiberDiplomacia).

Nye (2010) sustenta a teoria acima referida, afirmando que:

> *"Power based on information resources is not new; cyber power is. There are dozens of definitions of cyberspace but generally "cyber" is a prefix standing for electronic and computer related activities. By one definition: "cyberspace is an operational domain framed by use of electronics to …exploit information via interconnected systems and their associated infra structure." Power depends on context, and cyber power depends on the resources that characterize the domain of cyberspace(…)In terms of soft power, an individual or organization might attempt to persuade others to change their behavior. The Chinese government sometimes used the internet to mobilize Chinese students to demonstrate against Japan when its officials took positions that offended Chinese views of the 1930s relationship. Al Qaeda videos on the internet designed to recruit people to*

*their cause are another case of Soft Power being used to change people from their original preferences or strategies*" (Nye, 2010, p. 3-6).

O autor defende ainda que os instrumentos de informação podem ser utilizados para produzir Soft Power no Ciberespaço através do enquadramento da agenda, de métodos de atração ou de persuasão, por sua vez e relativamente aos recursos potencializadores de Soft Power e os investimentos que estes requerem, os governos podem estabelecer servidores e softwares projetados para apoiar ativistas de direitos humanos e dar uma outra visibilidade às suas mensagens, servidores e softwares projetados para ajudar ativistas de direitos humanos a propagar as suas mensagens, temos como exemplo desta situação a sequência de repressões ocorridas depois da eleição de 2009 por parte do governo iraniano, os EUA investiram em programas (softwares e hardwares) que facilitaram a divulgação de informação e mensagens pelos manifestantes (Nye, 2008).

É possível afirmar que o "Ciber"- Soft Power, funciona como uma extensão do Soft Power e respetivas ferramentas no Ciberespaço e deste modo, a noção de Soft Power aliada ao prefixo "ciber", surge como a capacidade de influenciar, de controlar ou dominar os recursos existentes no Ciberespaço com uma finalidade que não se limita apenas ao Estado e ao seu interesse nacional/internacional, mas também a outros atores civis ou não. Iniciativas de Soft Power e esforços diplomáticos têm conseguido atingir os resultados esperados um pouco por todo o mundo, pois é possível concluir que quando um sujeito define determinado objetivo, torna-se fácil traçar todo um caminho fiel para alcançar o seu resultado final, seja ele uma posição, ideologia ou proposta que influenciará outros a apoia-la/segui-la.

Complexo e simultaneamente simples, sabemos que não existe substituto para a interação direta e pessoal, vulgarmente chamada de "cara a cara", mas precisamos abraçar o fato de que a informação que consumimos diariamente molda as nossas visões do mundo, as nossas opiniões e perspetivas e que aqueles que ganham o debate digital têm uma chance melhor de criar um discurso dominante (Freitas, Silva e Teixeira, 2015), no caso da Ciberdiplomacia como veremos nos capítulos seguintes, continuará a ser uma componente chave no que diz respeito às estratégias da Diplomacia com elevado potencial de se tornar numa ferramenta chave de politica externa, no entanto não podemos negligenciar o elemento humano que nela consta: os componentes emocionais e

ideológicos que fazem parte da forma como utilizamos o Ciberespaço e interagimos online, e corremos o risco de cair na armadilha do determinismo tecnológico, ou seja permitir que a tecnologia de uma sociedade impulsione o desenvolvimento das suas estruturas sociais e valores culturais e não o contrário.

Como podemos verificar, se a Diplomacia se constitui como uma forma de Soft Power e se transferirmos essa Diplomacia para o Ciberespaço, chegamos a um "ciber" Soft Power, que nada mais é do que o poder brando no Ciberespaço como por exemplo a Ciberdiplomacia, que como veremos mais adiante se trata de uma ferramenta crucial na segurança do Ciberespaço europeu.

Como também é possível observar no capítulo anterior e como será aprofundado, a Ciberdiplomacia (ferramenta de Soft Power) por si só não se traduz numa estratégia eficaz de Cibersegurança, no entanto, aliada a outras ferramentas torna-se crucial e indispensável para o bom funcionamento da Cibersegurança na UE e para a gestão e prevenção de conflitos, não só na união como no mundo.

# 3.Cibersegurança na UE

A Cibersegurança constitui-se como parte integrante da segurança dos europeus. Mais do que nunca, a economia, a democracia e a sociedade na UE estão dependentes de ferramentas e ligações digitais que devem ser seguras e confiáveis. A Cibersegurança afigura-se, portanto, essencial para construir uma Europa resiliente, ecológica e digital (Comissão Europeia, 2020).

Uma vez que como veremos adiante a Ciberdiplomacia se constitui como uma ferramenta eficaz e potente enquadrada nas estratégias de Cibersegurança existentes é importante analisar de uma forma geral quais os acontecimentos mais marcantes na questão de Cibersegurança da UE, bem como a legislação existente desde sempre, o que realmente tem sido posto em prática e como nos últimos 20 anos no caso europeu.

Mueller (2017) afirma que a Ciberdiplomacia oferece o potencial para diminuir os conflitos no Ciberespaço e, portanto, constitui-se como uma força pela paz.

A escolha da União Europeia como objeto de estudo prende-se pelo facto desta ser uma instituição bastante capacitada a nível de segurança e com um sistema global de gestão de crises que promove a estabilidade internacional trabalhando não só dentro como fora das suas fronteiras.

Sabemos que a proteção dos cidadãos da UE se encontra dependente de uma ação conjunta de todos os seus  Estados Membros, não sendo possível alcançar a mesma por meio de ações isoladas dos seus membros, assim e de acordo com o comunicado da Comissão Europeia relativo à Estratégia de segurança da UE (2020) é indispensável trabalhar em conjunto para tirar proveito dos pontos fortes da UE e assim fazer a diferença, uma vez que é sabido que a responsabilidade pela segurança de cada país parte dele mesmo, não deixa de ser evidente que a segurança de um Estado Membro se encontra relacionada com a segurança de todos os outros Estados Membros e que neste âmbito e de acordo com Brandao (2010), a UE permite responder de forma integrada e multidisciplinar ajudando os seus intervenientes nos domínios da segurança e do Ciberespaço através não só de instrumentos como de informações que estes necessitem.

A UE permite assim assegurar que as suas estratégias e politicas de segurança se mantenham assentes nos valores comuns europeus (Bindi, 2010), e que a segurança, confiança, direitos

e liberdades dos seus cidadãos sejam assegurados e bem protegidos, e é desta esta capacidade e influência que UE apresenta para a segurança internacional e mais especificamente para a Cibersegurança, que o Soft Power ganha forma promovendo de acordo com Duke e Ojanen (2006) mudanças a nível político e a nível de mitigação de conflitos.

A Ciberdiplomacia no sentido mais amplo abrange medidas de construção de confiança e cooperação e também inclui certos aspetos da construção de normas internacionais, proteção de dados, liberdade de expressão, governança da Internet e processos judiciais sob acordos internacionais por não fornecer assistência jurídica mútua, daí ter um papel tão importante nas estratégias de Cibersegurança da UE.

## 3.1 Instrumentos jurídicos

No caso específico da UE que é o foco desta dissertação, e de acordo com Fuster e Jasmontaite (2020) é relevante em termos jurídicos, no caso da Cibersegurança, ressaltar a Diretiva SRI e o Regulamento da Cibersegurança da UE, como bases legislativas do Ciberespaço europeu.

A Diretiva SRI entrou oficialmente em vigor em julho de 2016, sendo que a mesma viu a sua origem na Comunicação da Comissão Europeia de 2009 focada na prevenção e consciencialização, delimitando um plano de ação imediata com medidas que promovem o reforço da segurança no Ciberespaço. A Diretiva SRI, constitui-se como o pilar central da Estratégia para a Cibersegurança de 2013 (referida anteriormente na presente dissertação) e constitui-se também como o primeiro ato legislativo da UE em matéria de Cibersegurança e abrange todos os Estados Membros. Em termos estruturais, a Diretiva SRI encontra-se organizada em sete capítulos e vinte e sete artigos e analisando o Artigo 27º, é de ressaltar o nº3, que identifica as motivações centrais e o respetivo âmbito de atuação conforme o seguinte:

> *"As redes e os sistemas de informação e, sobretudo, a Internet desempenham um papel crucial para facilitar a circulação transfronteiriça de mercadorias, de serviços e de pessoas. Devido a essa natureza transnacional, as perturbações significativas desses sistemas, intencionais ou não, e independentemente do local onde ocorram, podem*

*afetar os Estados Membros, individualmente considerados, e a União no seu conjunto. Por consequência, a segurança das redes e dos sistemas de informação é essencial para o bom funcionamento do mercado interno."* (Diretiva SRI (UE) 2016/1148, 2016, artigo 1 e 3).

Relativamente aos sete capítulos nos quais se divide a Diretiva: os três primeiros capítulos tratam dos efeitos da diretiva polivalente e das respetivas obrigações decorrentes das suas disposições, nos capítulos quatro e cinco, as obrigações dos Estados Membros em relação à estratégia nacional, bem como a cooperação a nível da UE, enquanto o papel essencial da ENISA na implementação da Diretiva SRI (conforme reforçado pela proposta do novo Regulamento da ENISA, a Lei de Cibersegurança da UE) é apresentado no sexto capítulo. Consequentemente, a Diretiva SRI propõe a criação de um mecanismo de resposta a incidentes suscetíveis de prejudicar serviços essenciais, permitindo o funcionamento normal da sociedade e do mercado interno, e visa definir medidas para atingir um elevado nível comum de Cibersegurança na União Europeia (artigo 1. º). No entanto, de acordo com Kasper e Antonov (2019) e tendo em conta que o referido propósito poderá não ser alcançado na sua totalidade, e que poderá apresentar um âmbito mais vasto a nível da UE, através de medidas adotadas de acordo com o princípio da subsidiariedade e da proporcionalidade. incluída no artigo 5. º do Tratado da União Europeia (TUE). Para atingir este objetivo, a presente diretiva estabelece o seguinte:

*a)* Obrigatória por parte dos Estados Membros na adoção de estratégias nacionais para redes e sistemas de informação (artigo 7º);
*b)* Criação de grupos de cooperação para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros e criar confiança entre eles (artigo 11º);
*c)* Criar uma rede de equipas de resposta a incidentes de segurança informática para ajudar a criar confiança entre os Estados-Membros e promover uma cooperação operacional rápida e eficiente (artigo 12º);
*d)* Estabelecimento de requisitos de segurança e notificação para operadores de serviços essenciais (artigo 14 º) e para fornecedores de serviços digitais (artigo 16º);
*e)* Definir a obrigação dos Estados-Membros designarem autoridades nacionais

competentes, balcões únicos e CSIRT com competências relacionadas com a segurança das redes e dos sistemas de informação (artigos 8 º, 9 º e 10 º).

A Diretiva estabelece ainda que de forma a determinar a gravidade de um ciberataque, devem ser considerados parâmetros como o número de usuários afetados pela situação, a duração do ciberataque, a localização e abrangência geográfica, o grau de perturbação causado e a influência do incidente na economia e na sociedade (Kasper e Antonov, 2019).

> *"É interessante notar que, embora as duas estratégias de Cibersegurança da UE tenham seguido a adoção de inúmeras medidas legislativas relativas à Cibersegurança, foram colocados objetivos de política que posteriormente resultaram em legislação, nomeadamente a Diretiva de Segurança de Redes e Informações (SRI) e a Lei de Cibersegurança, que esclarecem ainda mais o papel e o mandato da Agência da União Europeia para Redes e Segurança da Informação (ENISA)"* (Fuster e Jasmontaite, 2020, p.101).

A ENISA localiza-se na Grécia (Heraklion Creta) e possui um escritório operacional em Atenas. Fundada através do Regulamento (CE) nº. 460/200453, desde 2004, que a ENISA tem sido um ator ativo na promoção da segurança na EU, e a sua missão passa sobretudo por aumentar:

> *"a sensibilização para as redes e a segurança da informação e desenvolver e promover uma cultura de segurança das redes e da informação na sociedade em benefício dos cidadãos, consumidores, empresas e organizações do setor público da União"* (Regulamento ENISA (UE) 526/2013, 2013, artigo 1º).

Na prática, relativamente aos fornecedores de serviços digitais, a ENISA emitiu um relatório para ajudar os Membros da UE no âmbito de proporcionar aos fornecedores de serviços digitais uma abordagem comum com medidas de segurança mínimas, o objetivo do relatório passa por definir uma referência de segurança comum.

O Regulamento 881/2019 da UE alusivo à Cibersegurança, aprovado a 17 de abril de 2019 pelo Parlamento e o Conselho Europeu, diz respeito a um novo conjunto de normas da

Agência da União Europeia para a Cibersegurança (ENISA) e à criação de um quadro de certificação a nível da UE. O objetivo é garantir o bom funcionamento do mercado interno e, ao mesmo tempo, a obtenção de um elevado nível de Cibersegurança. O presente regulamento estabelece por um lado os objetivos, funções e aspetos organizacionais da ENISA, e por outro a definição de um Quadro para o estabelecimento de sistemas europeus de certificação da Cibersegurança.

A ENISA criada com o regulamento 881/2019 sucede à ENISA criada com o regulamento n. 526/2013, tendo este sofrido melhorias no sentido da consciencialização da UE no âmbito da Cibersegurança que tem vindo a ganhar cada vez mais destaque uma vez que este novo regulamento transforma a ENISA numa agência permanente de Cibersegurança, define as suas competências, a sua estrutura organizacional, regras de funcionamento, regime orçamental, pessoal e métodos de desenvolvimento e acompanhamento do trabalho da agência. Além disso, o regulamento institui o grupo de interessados pela certificação da Cibersegurança (artigo 22º), co-presidido pela ENISA e cujo secretariado é garantido pela agência, composto por peritos a selecionar através de concurso transparente e aberto, que terá a função de aconselhar a Comissão sobre questões estratégicas relacionadas com o quadro europeu para a certificação da Cibersegurança e na preparação do programa de trabalho em curso da UE para a certificação europeia da Cibersegurança (artigo 47 º).

A UE tem tomado medidas para reforçar o papel da ENISA (Pinto, 2019) de modo a garantir que o nível de Cibersegurança se mantém elevado e para ajudar os Estados Membros a implementar uma política de segurança nacional eficiente para esse fim e neste sentido a Diretiva SRI pode ser vista como uma resposta tardia a um problema já exacerbado e conhecido de acordo com Fuster e Jasmontaite (2020), até ao presente momento,as ciberameaças e os ciberataques em si não foram apenas identificados ao nível de especialistas, mas muitas vezes chamaram a atenção dos mídia e das redes sociais. Os instrumentos jurídicos dos quais a UE dispõe nesta vertente oferecem uma resposta bem conseguida e estruturada que tem em conta a problemática em questão e os planos para o futuro e neste âmbito é importante ressaltar a Ciberdiplomacia, e considerando a decisão (PESC) 2019/797 do Conselho, ( Maio de 2019), é nos possível concluir e de acordo com Pinto (2019) que em Junho de 2017, foram adotadas conclusões pelo Conselho relativas ao quadro de resposta conjunta no âmbito diplomático da UE contra as atividades

maliciosas do Ciberespaço, denominada "instrumentos de Ciberdiplomacia", onde se manifestou preocupação geral por parte da UE com a crescente capacidade dos intervenientes (estatais e não estatais) recorrerem a atividades cibermaliciosas para alcançar os seus objetivos afirmando a necessidade de proteger a integridade e segurança da UE no Ciberespaço e neste âmbito em outubro de 2017, foram aprovadas pelo Comité Político e de Segurança, orientações de execução para o conjunto de instrumentos de Ciberdiplomacia, onde se destacam o reforço da resposta diplomática da UE aos ciberataques, a promoção da resiliência, a procura de meios de combater a cibercriminalidade, o fomento da Ciberdiplomacia e reforço da ciberdefesa e a atribuição do regime de sanções.

## 3.2 Cibersegurança na UE: análise dos últimos 20 anos

Como já visto anteriormente, a Cibersegurança é a prática de proteger sistemas críticos e informações confidenciais de ciberataques. Também conhecida como segurança das tecnologias da informação (TI) (Jorge e Wendt, 2013), as medidas de Cibersegurança são projetadas para combater ameaças contra sistemas e aplicativos em rede, sejam essas ameaças provenientes de dentro ou de fora de uma organização.

> *"A par dos pilares tradicionais (terra, ar e mar) é hoje consensual que o pilar digital é tão relevante como os demais, princípio que ficou consagrado na Cimeira da NATO de 2014, em Gales. Mas diríamos que este (...) abarca ainda, além das questões de segurança, a questão da liberdade da internet, do livre fluxo de dados (free flow of data) e dos meta-dados, questões que vão merecer atenção crescente da comunidade internacional nos próximos anos."* (Alves, 2021, p.119).

O deputado assume que o mundo virtual ganha tanta importância como o mundo físico, no entanto que este acaba por trazer consigo aspetos mais complexos que vão além das questões de segurança e que requerem a atenção internacional, o que faz bastante sentido tendo em consideração que é um campo de ínfimas possibilidades e de grandes desafios

a nível social, económico, político, cultural, tecnológico e militar, e que oferece uma vasta gama de oportunidades, porém simultaneamente permite o aparecimento de ameaças capazes de afetar tanto a privacidade e segurança dos cidadãos comuns como as infraestruturas críticas de um Estado.

Relativamente às ações conduzidas pela União Europeia e segundo Alves (2021), nos termos do Tratado de Maastricht, e devido à importância TIC, questões alusivas à segurança do Ciberespaço enquadraram-se no primeiro pilar, o que por um lado permitiu que a UE desse inicio a uma legislação e se envolvesse de forma ativa no processo de tomada de decisão do plano internacional.

Este foco na Cibersegurança segundo Čelik (2019) deu início à proposta da Comissão Europeia de uma Estratégia de Cibersegurança em 2001, sendo este o primeiro documento representativo de uma política de Cibersegurança na UE, documento que é um marco a diversos níveis no que diz espeito à politica de Cibersegurança, pois nele constam detalhadamente as ciberameaças e respetivas medidas de segurança.

A Proposta de 2001 expôs a vertente económica da Cibersegurança e destacou a importância da justiça criminal, como resultado duas novas agências foram estabelecidas para realizar as operações de política: Europol, na qual um novo departamento foi criado em 2002, denominado "Centro de crime de alta tecnologia", e a ENISA que iniciou as suas operações em 2004 em Heraklion na ilha de Creta como umcentro de especialização em segurança de rede e informação para a UE (Čelik, 2019), respetivos Estados Membros, o sector privado e os cidadãos europeus.

Com os ataques já referidos que visaram a Estónia em 2007 e outros, a UE ganhou um novo interesse pela temática da ciberesegurança (Tikk, Kaska e Vihul, 2010), e como consequência, entre os anos de 2007 e 2013, e de acordo com Pinto (2019) houve um aumento significativo de documentos legais relacionados com a Cibersegurança, o que contribuiu para o fortalecimento das medidas de Cibersegurança. A União Europeia iniciou os regulamentos de Cibersegurança na área de proteção das infraestruturas críticas em 2009, concentrando-se na proteção da Europa contra ciberameças, aumentando a segurança e a resiliência. A comunicação lançou um plano de ação, envolvendo também os Estados Membros e o setor privado, o qual assentava em cinco pilares que se baseavam na prevenção e preparação prévia de conflitos, na capacidade de resposta e deteção dos mesmos, na recuperação, na cooperação internacional e na definição de critérios no

domínio das TIC a nível europeu.

No mesmo ano, o Conselho da União Europeia destacou a necessidade de desenvolver sistemas de TIC resilientes e seguros e a necessidade de atualizar as competências técnicas da Europa. Duas conferências foram realizadas, (Tallinn, 2009 e Balatonfured, 2011) o que conduziu à adoção da Resolução do Parlamento Europeu sobre a proteção de infraestruturas críticas de informação, a criação do Fórum Europeu dos Estados Membros e da Parceria Público-Privada Europeia para a Resiliência; dois exercícios pan-europeus (Cyber Europe 2010 e 2012); recomendação de política pela ENISA sobre um conjunto mínimo de recursos e serviços básicos; e recomendações sobre o funcionamento dos CERTs (equipas de resposta a emergências computacionais) nacionais (Pinto, 2019).

Segundo Deward (2017) uma resposta para a crise financeira de 2008 que assolou a europa teve como base a identificação da necessidade de estabelecer novos estímulos em certos setores industriais, que promovessem o crescimento económico e o aumento das taxas de empregabilidade, sendo o domínio digital um dos principais focos. Como resultado,é iniciada uma Agenda Digital para a Europa, destinada a aumentar a absorção da tecnologia digital em todos os setores da sociedade - política, social e económica - e transformar a UE numa sociedade baseada no conhecimento económico.

Com o Tratado de Lisboa, em 2009, a noção de pilares foi abolida (Teixeira, 2010). Assinado em 2007, e em vigor desde 2009, o Tratado de Lisboa modificou a PESC, proporcionando melhorias no âmbito do quadro legal em vigor que passou a ser mais favorável à UE, e à sua atuação no sistema internacional (Pinto, 2019). O Tratado de Lisboa acarretou vários feitos relevantes tais como a criação do cargo de Alto Representante para Negócios Estrangeiros e Política de Segurança (nova designação atribuída ao cargoda UE anteriormente designado como Alto Representante para a PESC) que deveria direcionar a PESC e representar a UE como voz singular (Brandão, 2010); a introdução da PCSD que sucedeu à PESD, mais vasta e com o objetivo de organizar uma Defesa europeia comum; a criação do SEAE, como estrutura de apoio ao Alto Representante que compreendia um conjunto de órgãos, nomeadamente da Comissão, da rede de Delegações Externas da UE, do Estado Maior Militar, de uma Direção Civil-Militar de Gestão de Crises, de um Centro de Situação, de uma Direção de Ação Policial, entre outros (Pinto, 2019).

O Tratado de Lisboa demonstra a importância da Cibersegurança, ao mencionar especificamente a mesma no artigo 69.º como uma área que requer cooperação para apoiar

a  estabilidade do mercado interno.

Os processos de formulação e alterações de políticas começaram no início de 2007, fortalecidos pelo Tratado de Lisboa e apresentaram o seu auge no desenvolvimento da Estratégia de Cibersegurança da União Europeia - seguindo um longo e controverso processo de negociação e com o objetivo central de construir uma Cibersegurança resiliente para manter o *status quo* global simultaneamente mantendo-se disponível a novos desafios. A estratégia enfatiza a unidade das autoridades públicas e do setor privado, bem como o desenvolvimento do Ciberespaço e respetivas capacidades, recursos e eficiência (Kovac, 2018). De modo a persuadir este objetivo, tornou-se necessário um sistema de prevenção, deteção e gestão a nível da UE e assim surge em 2016, a primeira parte da legislação do Ciberespaço que foi adotada pelo Parlamento Europeu: A proposta da Diretiva SRI.

A referida proposta é relativa à segurança de redes e sistemas de informação, no entanto e segundo Pinto (2019), foram necessários mais três anos para finalizar o documento e moldar ainda mais o papel da UE no Ciberespaço.

A Diretiva SRI estabeleceu um novo quadro institucional para impulsionar o nível geral de Cibersegurança na UE, no qual foram incluídos os seguintes critérios:

- Estados Membros passam a nomear uma autoridade SRI nacional e um CERT;

- Criação de uma rede de partilha de informações entre os membros da UE, e a rede de CSIRTs nacionais, para promover uma cooperação rápida e eficiente;

- A construção de uma cultura de segurança em todos os setores vitais para a economia e sociedade e para aqueles que dependem fortemente das TICs, como energia, transporte, água, bancos, infraestruturas do mercado financeiro, saúde e infraestrutura digital;
- As empresas nestes setores que são identificadas pelos Estados Membros como operadoras de serviços essenciais terão que ter a segurança adequada, bem como medidas adequadas e notificar incidentes graves à autoridade nacional competente.

- Os principais provedores de serviços digitais deverão cumprir com a segurança e requisitos de notificação ao abrigo da nova diretiva.

É então possível afirmar que a Diretiva SRI é a pedra angular da resposta da UE às ciberameaças crescentes e aos desafios que acompanham a digitalização da vida económica e social.

Ainda em 2016, é revisto o Regulamento (UE) n.º 526/2013do Parlamento Europeu e do Conselho Europeu no que se refere à ENISA revogando o Regulamento (CE) n.º 460/2004, no qual o objetivo da avaliação passa pela reforma da ENISA, reforçando o funcionamento da mesma, as suas capacidades e os instrumentos de apoio aos Estados Membros. Em 2017 e de acordo com Kováks (2018), foi adotada uma nova Estratégia de Cibersegurança, foi o chamado "ato de Cibersegurança", que trouxe duas mudanças: por um lado, uma reforma abrangente da ENISA e por outro, a criação de uma estrutura de certificação neste âmbito. Simultaneamente o Conselho da UE concordou em desenvolver um quadro para uma resposta diplomática conjunta da EU a atividades duvidosas no Ciberespaço - a caixa de ferramentas de Ciberdiplomacia e relativamente à caixa de ferramentas de Ciberdiplomacia, o quadro da resposta diplomática conjunta da UE faz parte da abordagem da mesma em relação à Ciberdiplomacia, que contribui para a prevenção de conflitos, para a atenuação das ameaças à Cibersegurança e uma maior estabilidade nas Relações Internacionais.

Espera-se que a estrutura incentive a cooperação, facilite a mitigação de ameaças imediatas e de longo prazo e influencie o comportamento de potenciais agressores a longo prazo, no fundo o que se espera, é que a mesma incentive a prevenção e mitigação de conflitos no Ciberespaço, uma vez que a resposta diplomática da UE a ciberameaças fará pleno uso de medidas de Ciberdiplomacia presentes no âmbito da PESC.

O ideal será conseguir uma resposta conjunta da UE às ciberameaças proporcional ao impacto das mesmas, tendo em consideração que a UE está empenhada em resolver litígios no Ciberespaço internacional de forma pacífica e que o objetivo principal da UE deverá ser a promoção de segurança e estabilidade através de esforços diplomáticos e de uma maior cooperação internacional que permita reduzir em grande escala o risco de acontecimentos maliciosos derivados da utilização das TIC.

A UE de acordo com o Conselho Europeu (2019) reconhece que o Ciberespaço oferece oportunidades significativas, mas também coloca desafios em constante evolução para a

ação externa da mesma. A UE está preocupada com o aumento da capacidade e da vontade dos atores estatais e não estatais de perseguir os seus objetivos através de atividades maliciosas no Ciberespaço, atividades que podem constituir atos ilícitos ao abrigo do direito internacional e podem originar uma resposta conjunta da UE, que reitera que os Estados não devem permitir intencionalmente que o seu território seja utilizado para atos internacionalmente (Conselho Europeu, 2019).

Em 2019, surge uma nova Estratégia, que continuou a reforçar legalmente o Ciberespaço europeu e no ano de 2020, é apresentada a nova Estratégia de Cibersegurança,que procura responder aos desafios de competição geopolítica no Ciberespaço, e às ciberameaças cada vez maiores, especialmente durante a pandemia covid-19.

Em Dezembro de 2020 com a nova Estratégia da UE para a Cibersegurança, foram apresentadas propostas pelo Alto Representante com o intuito de prevenir e reagir de forma eficaz contra as ameaças no Ciberespaço.

A UE tenta ainda reforçar a cooperação no campo da ciberdefesa e definir estratégias eficazes nesta área segundo o trabalho que tem vindo a ser realizado pela Agência Europeia de Defesa e procura também incentivar à cooperação dos Estados Membros, reforçando o conjunto de ferramentas de Ciberdiplomacia e intensificando as medidas para desenvolver a capacidade da mesma (Ciberdiplomacia) em países terceiros.

Um dos objetivos da UE passa também por promover a sua visão no Ciberespaço através da construção de uma rede global de Ciberdiplomacia. A nova estratégia permite à UE aumentar a sua resiliência e mostrar liderança no Ciberespaço, desenvolver capacidades para prevenir, deter e responder aos ciberataques e fortalecer as suas parcerias em prol de um Ciberespaço global e aberto, (dados do Serviço Europeu de Ação Externa, 2020).

É ainda no ano de 2020 que UE impõe as primeiras sanções contra ciberataques*:*

> *"O Conselho decidiu hoje impor medidas restritivas contra seis pessoas e três entidades responsáveis por vários ciberataques ou que neles participaram. Trata-se, nomeadamente, da tentativa de ciberataque contra a OPAQ (Organização para a Proibição de Armas Químicas) e dos ciberataques publicamente conhecidos como "WannaCry", "NotPetya", e "Operation Cloud Hopper"* (Conselho Europeu, 2020, p.1).

Feito que se constitui como um grande passo no papel de Ciberdefesa e Ciberdiplomacia da UE para a prevenção e proteção do Ciberespaço europeu.

Mueller (2017) afirma que a Ciberdiplomacia oferece o potencial para diminuir os conflitos no Ciberespaço e, portanto, constituir-se como uma força pela paz. Mais de trinta estados agora têm comissários para a política externa do Ciberespaço sendo que a Dinamarca até nomeou um embaixador para a Ciberdiplomacia.

A Ciberdiplomacia no sentido mais amplo abrange medidas de construção de confiança e cooperação e também inclui certos aspetos da construção de normas internacionais, proteção de dados, liberdade de expressão, governança da Internet e processos judiciais sob acordos internacionais por não fornecer assistência jurídica mútua. Muitos governos, no entanto, não têm o conhecimento nem os recursos necessários para manter os padrões básicos de Ciberdiplomacia ou mesmo para verificar os ataques que são conduzidos através de servidores no seu território (daí a importância da união de todos os Estados Membros da UE).

## 3.3 Ferramentas da UE no combate às ciberameaças

Relativamente à problemática das ciberameaças e do cibercrime, esta constitui especial importância pois apesar da Ciberdiplomacia não atuar diretamente nessa área a mesma apresenta um papel chave fundamental como medida preventiva uma vez que como iremos verificar a Ciberdiplomacia não se constitui por si só como uma ferramenta de combate ao cibercrime, no entanto através das suas ferramentas de negociação pacífica é possível apaziguar conflitos e prevenir a ocorrência dos mesmos, logo é uma ferramenta capaz na prevenção de ciberameaças e de algumas potenciais ocorrências criminosas no Ciberespaço, reforçando de acordo com a Comissão Europeia (2020), a resposta diplomática da UE aos ciberataques.

De acordo com a Comissão Europeia (2020), o termo "cibercrime" nada mais é do que ações criminosas cometidas no ciberespaço (online) com recurso às TIC e sistemas de rede e nesse sentido a UE implementou leis e apoia a cooperação não só diplomática como operacional através de ações não legislativas e financiamento, o cibercrime é uma

questão sem fronteiras que a Comissão Europeia (2020) classifica segundo as seguintes definições:

- Crimes específicos do Ciberespaço, tais como phishing ou ciberataques contra sistemas de informação (por exemplo, sites falsos para solicitar senhas que permitem o acesso aos dados privados das vitima);

- Crimes de índole fraudulenta e de falsificação no Ciberespaço (roubo de dados, roubo de identidade, SPAM, entre outros).

- Conteúdo ilegal no Ciberespaço, o que inclui conteúdo relacionado à pedofilia, incitação ao ódio, aos atos terroristas e à violência, entre outros.

Muitos tipos de crime, incluindo os mencionados acima, têm vindo a ganhar território online o que obriga a que a maioria das investigações trabalhe também com um pé assente no Ciberespaço, e as leis e ações da UE de modo a dar resposta ao cibercrime visam sobretudo melhorar a prevenção, investigação e ação penal contra cibercrimes e melhorar a aplicação das leis e no judiciário trabalhar com a indústria para capacitar e proteger os cidadãos.

A criptografia é considerada uma forma eficaz de garantir a proteção da Cibersegurança, a proteção de dados e a privacidade. Pode ajudar os cidadãos e as empresas a protegerem-se contra o abuso de tecnologias de TI, como hacking, roubo de identidade e dados pessoais, fraude e divulgação indevida de informações confidenciais, a criptografia também pode ser usada por criminosos para ocultar as suas ações das autoridades o que acontece na maioria dos casos de ciberataques e cibercrimes, o que dificulta o acesso legal a provas eletrónicas importantes e torna o trabalho das autoridades mais desafiantes e complicados de investigar (Conselho Europeu, 2020).

Operações conduzidas por determinado países contra Estados e instituições da União Europeia (e de outros atores internacionais) têm aumentado significativamente em dimensão e escala, diversas operações no Ciberespaço têm de forma "discreta" minado a estabilidadedo Mercado Único Digital através de ciberespionagem, eliminação e cópia de dados e ataques disruptivos (Moret, 2017), atividades que podem constituir atos ilícitos ao

abrigo do direito internacional e podem desencadear uma resposta conjunta da UE e é nesta vertente que a estratégia da UE para um Ciberespaço seguro, aberto e protegido ganha destaque.

Inicialmente, a estratégia de Cibersegurança da UE centrou-se em manter o Ciberespaço aberto, livre, estável e seguro. (Conclusões do Conselho em 2017). No ano de 2012, Catherine Ashton, afirmou que a vulnerabilidade das nossas sociedades está fadada a atrair forças destrutivas. Conforme verificado anteriormente, a Estratégia de Cibersegurança da UE de 2013 (EUCSS) visava harmonizar a prontidão dos países da UE na forma como reagiriam com os desafios de Cibersegurança, tendo sido atualizada em 2017 com o intuito de aumentar o nível de proteção e segurança das infraestrutura críticas da União Europeia e foi nesse mesmo ano que a Comissão Europeia criou uma base sólida para uma estratégia de combate ao cibercrime na qual foram formuladas várias medidas e políticas para o Ciberespaço que incluíram disposições sobre um mandato permanente para a ENISA, um quadro que permite certificar a Cibersegurança na UE, implementar na totalidade da Diretiva SRI, um plano para resposta rápida de emergência; criação de centros de ciberpesquisa na UE; melhorias na resposta a aplicar e aumento da resiliência geral da União Europeia.

O ritmo com que estas iniciativas foram aprovadas mostra que a UE tem maturidade suficiente para reconhecer os perigos do Ciberespaço e agir sobre eles. Se, por um lado, a Comissão Europeia está a tomar medidas para proteger o Mercado Único Digital, por outro, os Estados Membros no Conselho mantêm as prerrogativas nacionais.

Relativamente às capacidades militares, os países da UE ainda se encontram um pouco limitados, de acordo com a Conferência de Segurança de Munique, 2019, existiam à data cerca de 2.500 a 3.500 soldados nas forças de Cibersegurança europeias com diferenças significativas entre os países em termos de capacidade nacional. O número é baixo quando comparado ao tamanho do US Cyber Command, que é cerca de duas vezes maior e deveria crescer substancialmente em 2019 (Breene, 2016) e partindo destas estimativas, parece evidente que existe uma certa lacuna capacidade-expectativa na ciberdefesa da UE.

Desde o início da formulação de políticas da UE em matéria de Cibersegurança, o quadro ciberinstitucional da UE evoluiu para um sistema descentralizado governado pelos Estados Membros. As instituições e agências apoiam o desenvolvimento de capacidades

garantindo a consistência entre os Estados Membros e facilitando a coordenação e divulgação (Barrinha e Carrapiço, 2017), no entanto, torna-se difícil dissuadir os agentes maliciosos das suas ciberatividades, e desafios como este aliados à falta de meios para apoiar a estratégia da UE no Ciberespaço facilitam os cibercriminosos a perpetuar os seus ciberataques incentivando a proliferação dos mesmos. Neste contexto e indo de encontro à questão de pesquisa deste trabalho é claro que a Ciberdiplomacia não se constitui por si só como uma ferramenta de combate ao cibercrime, no entanto através desta forma de negociação pacifica é possível apaziguar conflitos e prevenir a ocorrência dos mesmos, como defendem os autores Barrinha e Renard (2017), a UE utiliza recursos e funções diplomáticas para projetar e coordenar os interesses dos seus Estados Membros no Ciberespaço e a Ciberdiplomacia como veremos mais adiante faz parte da estratégia da UE no combate às ciberameaças, o seu objetivo passa por influenciar o comportamento dos cibercriminosos sinalizando-lhes que as suas ações ilegais terão consequências (Nye, 2017). A UE também pretende chegar a um consenso internacional para promover um comportamento responsável no Ciberespaço.

Nas Conclusões do Conselho sobre Ciberdiplomacia em 2015, foi definido pelos Estados Membro o propósito de desenvolver uma política do Ciberespaço internacional coerente e eficaz que promovesse os interesses da UE a vários níveis, desde políticos a económicos e estratégicos e que simultaneamente mantivesse o estabelecimento de contactos com os parceiros principais, organizações internacionais, sociedade e setor privado (Secretariado-Geral do Conselho, 2015).

Para diminuir a probabilidade de ciberataques, a UE segue uma estratégia dupla, defendendo a sua postura normativa no cenário global e desenvolvendo uma estrutura diplomática para responder a estes ataques e ameaças (Kasper e Antonov, 2019):

- Em primeiro lugar, os Estados Membros da UE tomaram medidas para comunicar aos atores externos que as atividades maliciosas no Ciberespaço podem constituir atos ilícitos ao abrigo do direito internacional e dar origem a uma resposta conjunta da UE;

- Os Estados membros têm participado nas discussões das Nações Unidas sobre como aplicar as normas internacionais no Ciberespaço, no entanto, as discussões no Conselho de Segurança das Nações Unidas ficam estagnadas quanto ao problema da atribuição dosciberataques/ameaças a um sujeito ou entidade

especifico;

- A atribuição de ciberataques no Ciberespaço é dificultada pela arquitetura técnica e geografia da Internet, e pela discórdia geral entre os países sobre quais normas do direito internacional se aplicam ao Ciberespaço. Os países europeus aliaram-se aos EUA relativamente à comunicação e trocas de opiniões sobre o assunto, onde por um lado os EUA promoveram uma visão na qual o Direito Internacional Humanitário (DIH) se aplica ao Ciberespaço.

A Declaração do G7 de 2017 sobre o comportamento dos Estados responsáveis no Ciberespaço declarou que no interesse da prevenção de conflitos e da solução pacífica de controvérsias, o direito internacional também fornece uma estrutura para as respostas dos Estados a atos ilícitos que não equivalem a um ataque armado (G7: Reuniões de Ministros das Relações Exteriores, 2017). Segundo as disposições do DIH, ataques deliberados a civis são proibidos e, portanto, operações no Ciberespaço que não causem a perda de vidas ou destruição material ainda seriam ilegais, e neste sentido foram vários os especialistas académicos que apoiaram essa visão. Entre eles, Taddeo (2014) que tentou preencher o vazio conceitual existente ao redor da ciberguerra, argumentando que o Direito Internacional já contém as disposições necessárias para regulamentar o Ciberespaço.

Os custos de reputação podem dissuadir os atores estatais de levar a cabo ações no Ciberespaço, através da sua participação em diversos diálogos alusivos à questão do Ciberespaço a UE envia um sinal aos atores externos de que um determinado ataque pode prejudicar a reputação de um país no cenário internacional para além do impacto imediato que este tipos de incidentes causam (Nye, 2017).

Conforme verificado anteriormente, a União Europeia tem vindo a incentivar os Estados Membros a desenvolver determinadas estratégias de segurança do Ciberespaço. Esta lógica da União Europeia aliada á sua perceção de ameaças, impulsionou um conjunto diferenciado de instrumentos e instituições que permitissem alcançar os seus objetivos no Ciberespaço, mantendo uma abordagem normativa relativamente à internet e visando garantir os princípios base: liberdade, acesso e abertura para todos. (Christou, 2017).

De acordo com o autor Kozlowski (2018), o desenvolvimento de um sistema eficaz de

sanções contra ciberataques constitui um desafio para todos os atores políticos incluindo a UE e são vários os obstáculos a ser enfrentados, nomeadamente como atribuir os ataques a um agressor específico, como conseguir apresentar provas sobre a origem do ataque ou como influenciar os Estados Membros a impor sanções. São diversas as capacidades que a Comissão Europeia procura transmitir aos Estados Membros, incluindo a criação de um sistema relativo às questões de segurança das TIC dos Estados e embora pareça controverso à primeira vista, o desenvolvimento de simulações de ataques no ciberespaço e a implementação de linhas de apoio e denúncia direcionadas para conteúdos prejudiciais ou ofensivos, bem como a desenvolvimento de CERT' são algumas das estratégias propostas pela Comissão Europeia, ora, sendo a estratégia de Cibersegurança uma das prioridades da política europeia atual, foram criadas várias organizações com o intuito de proteger e garantir a segurança do Ciberespaço e dos utilizadores do mesmo.

Das instituições que se podem considerar relevantes para a execução de uma estratégiade Cibersegurança europeia e de acordo com Christou (2017), e Kasper e Antonov (2019) destacam-se a ENISA, a Agência Europeia de Defesa (EDA) e o Centro Europeu de Cibercrime (EC3), quanto às ferramentas da UE nesta vertente podemos destacar a Estratégia de Cibersegurança da UE de 2013, a Diretiva SRI de 2016 e o Quadro Conjunto de 2016 sobreo combate às ameaças híbridas constituem referências relevantes. Com o decorrer dos anos, a UE tem dedicado os seus esforços também à Ciberdiplomacia conforme temos verificado ao longo desta pesquisa, quer a nível multilateral quer a nível bilateral, a Estratégia de Cibersegurança da UE de 2013 foi um passo importante no desenvolvimento da Ciberdiplomacia da UE, uma vez que a mesma tem investido principalmente no aumento da prevenção, na resiliência e na coordenação de esforços. estabeleceu uma política para o Ciberespaço internacional coerente para a UE como uma das suas prioridades e de modo a agilizar o processo de troca de informações e de cooperação estratégica foi estabelecido o Grupo de Cooperação da Diretiva SRI, composto por representantes de Estados Membros, a Comissão Europeia a ENISA e a Rede CSIRTs (dedicada a compartilhar informações sobre ameaças em curso e cooperar em incidentes de Cibersegurança).

Têm sido desenvolvidos vários debates alusivos à temática da Cibersegurança entre a UE com vários países sendo que a parceria UE-EUA (na área da Cibersegurança) é uma das

mais desenvolvidas. Recentemente em 2017, foi proposto pela Comissão Europeia a criação de normas abrangentes relativas à Cibersegurança para promover a resiliência, a dissuasão e a resposta da UE nesta vertente.

Em 2018, a Comissão, o Parlamento e o Conselho (Europeus) chegaram a um consenso alusivo à questão da Lei de Cibersegurança, cujo objetivo passava por introduzir uma certificação de Cibersegurança a nível da UE, consolidar a ENISA e promover o desenvolvimento de redes de centros competentes em matérias de Cibersegurança, uma comunidade mais competente para estas questões e um centro europeu de Cibersegurança.

No ano de 2020 são impostas pela UE, as primeiras sanções contra ciberataques, e em Junho de 2021, a Comissão apresenta a sua visão de criar uma nova ciberunidade conjunta para lidar com o número crescente de ciberincidentes graves que afetam os serviços públicos e toda a União Europeia. Os ciberataques têm vindo a aumentar em número, escala e consequências, o que afeta gravemente a segurança da UE. Todos os atores relevantes na UE devem estar prontos para reagir em conjunto e trocar informações relevantes com base na "necessidade de compartilhar" e não apenas na "necessidade de saber". A ciberunidade conjunta proposta e anunciada pela primeira vez pela presidente Ursula von der Leyen, visa reunir os recursos e a experiência da UE na prevenção ciberameaças, ciberataques e responder com eficácia aos crimes.

Muitas vezes, as instituições que promovem a Cibersegurança, incluindo civis, polícia, diplomatas, ciberdefesa e parceiros do setor privado, trabalham separadamente e com a sua união, pretendem construir um setor físico e virtual que promova a cooperação das instituições da UE que previna e lute contra a cibercriminalidade terão, o que constitui uma etapa importante na conclusão do quadro europeu de para gerir crises de Cibersegurança, que aliada à resposta ciberdiplomática conjunta da União Europeia no âmbito das ciberameaças promove um comportamento responsável dos Estados no Ciberespaço, permitindo a utilização de toda a composição da PESC, incluindo as medidas restritivas, de prevenção, desencorajamento, dissuasão e reação relativamente a ciberatividades maliciosas. Segundo o Instituto de Estudos de Segurança da UE, (2019), a UE procura através de uma aplicação plena dos instrumentos regulamentares, da mobilização e da cooperação, fornecer apoio não só aos Estados Membros na defesa dos seus cidadãos, bem como dos seus interesses económicos e de segurança nacional

respeitando sempre os direitos e liberdades fundamentais e do Estado de direito.

Diversas comunidades, constituídas por redes, pelas instituições, orgãos e agências da EU, são responsáveis por prevenir, desincentivar, dissuadir e responder às ciberameaças, fazendo uso dos respetivos instrumentos e iniciativas tais como a ENISA, CSIRT entre outros.

Estas comunidades incluem , de acordo com a Comissao Europeia 2020:

- as autoridades de SRI, como as CSIRT, e a resposta a catástrofes;
- as autoridades policiais e judiciais;
- a CiberDiplomacia;
- a Ciberdefesa.

Dando relevo ao terceiro ponto apresentado acima que se traduz na Ciberdiplomacia, sabemos que no caso europeu esta procura essencialmente reforçar a resiliência conjunta da UE e aumentar as relações de confiança entre os Estados Membros, prevenir conflitos através da sua capacidade de encorajamento do diálogo e da cooperação o que contribui para uma diminuição das ameaças e desmoralização do comportamento doa agressores.

Neste âmbito (Ciberdiplomacia), é fundamental zelar por proteger os Direitos Humanos e promover o multilateralismo, incentivando o diálogo EU/Estados Membros e parceiros internacionais, e também através de medidas concretas e da implementação de projetos que apoiam os esforços dos países parceiros e das organizações internacionais, ao mesmo tempo que promove os seus próprios valores e interesses (Instituto de Estudos de Segurança da UE, 2019), a Caixa de Ferramentas da Ciberdiplomacia está no centro da resposta diplomática conjunta da UE às atividades maliciosas do Ciberespaço e o seu foco passa, como verificado acima por prevenir conflitos, mitigar ameaças à Cibersegurança e contribuir para uma maior estabilidade no Ciberespaço através de cinco conjuntos de medidas:

- Medidas de estabilidade, que englobam declarações politicas, conclusões do Conselho da UE, diligências diplomáticas, diálogos políticos e temáticos;

- Apoio da UE aos Estados-Membros, o que engloba a Cláusula de Solidariedade (Art. 222 TFUE) e Cláusula de Defesa Mútua (Art. 42.7 TEU);

- Medidas cooperativas, que se caraterizam pelas diligências da UE, assistência técnica e diálogos temáticos;

- Medidas preventivas que promovem o fortalecimento da confiança, ações de Diplomacia pública e campanhas de conscientização e a capacitação para o Ciberespaço;

- Medidas restritivas através de sanções direcionadas contra indivíduos e entidades.

Sabemos que a Cibersegurança na UE é composta por ferramentas e estratégias de combate às ciberameaças e cibercrime (Kasper e Antonov, 2019) e de ferramentas de gestão e prevenção de ciberameaças/conflitos, e é neste segundo grupo que a Ciberdiplomacia apresenta um papel bastante relevante uma vez que contribui para gerir e prevenir conflitos, logo contribui para um Ciberespaço seguro (Cibersegurança).

# 4. Ciberdiplomacia na UE

A Ciberdiplomacia constitui-se como uma ferramenta extremamente poderosa se implementada corretamente e através da cooperação de todos os Estados Membros.
Neste capítulo é estudado o processo evolutivo da Ciberdiplomacia permitindo entender como a Diplomacia se transformou, e analisar quais foram as causas que conduziram a essa mudança nos padrões tradicionais de execução da Diplomacia, bem como o impacto desta na esfera internacional e a perspetiva da mesma como ferramenta de gestão e prevenção de conflitos do Ciberespaço no caso europeu (conforme a questão de pesquisa).
A Ciberdiplomacia na União Europeia tem como objetivo desempenhar um papel no cálculo dos potenciais ataques e dos respetivos agressores, atuando como um dissuasor contra o mau comportamento, e embora o conjunto de ferramentas da Ciberdiplomacia seja um complemento das ações de Cibersegurança de cada Estado Membro, agir em conjunto permitirá que os Estados Membros aumentem a sua credibilidade e sucesso neste ramo, uma vez que respondendo às ciberameaças como ator unificado, a União Europeia terá uma melhor posição na defesa da sua segurança e dos seus interesses políticos e económicos.

## 4.1 Ciberdiplomacia na UE

Na história da humanidade, assistimos a saltos evolutivos significativos nas tecnologias utilizadas no registo da informação e também na comunicação, temos como exemplos primordiais o uso de documentos escritos em placas de argila, em papiro e, posteriormente, a criação da prensa tipográfica entre outros, até chegarmos à fase tecnológica.
As tecnologias incluem, por exemplo, escrever cartas, mensagens telegráficas, telefonia, comunicações sem fios, transmissões por satélite e comunicações por computador ou telemóvel e a evolução destas TIC ultimamente tem constituído enorme relevância no nosso quotidiano, uma vez que a maioria das pessoas as utiliza frequentemente para comunicar, divertir, informar. Aliás, atrever-me-ia até mesmo a afirmar que a vida como a conhecemos se tornaria (do ponto de vista comunicativo) impossível!
As formas de comunicação das quais dispomos tornam-se indispensáveis não só para trabalhar, como para tomar decisões, e a evolução do uso dessas tecnologias pela

Diplomacia, desde os tempos mais remotos e dos métodos mais rudimentares até à troca de mensagens pela Internet, deu um grande salto em direção aos relatórios fornecidos pelos diplomatas ou pelos seus representantes que têm a possibilidade de aceder a documentos e ficheiros de várias fontes e índoles, contendo não apenas informações escritas, mas também imagens, áudio e vídeo, em suma as TIC's mais modernas determinaram uma conectividade global efetiva (Gilboa, 2016) criando, no campo da Diplomacia, o que se convencionou chamar de Ciberdiplomacia, que atua no Ciberespaço através da internet que como verificado anteriormente se constitui como um dos principais canais de comunicação, permitindo a conectividade global, a prestação de diversos serviços e a troca de informações entre empresas, governos e particulares (Riordan, 2019), e esta tendência das nações se tornarem cada vez mais inteligentes acarreta a preocupação das autoridades para um modelo de conflito em que as suas ferramentas, capacidades de proteção e necessidades a vários níveis atuam sobre as suas infraestruturas de informações críticas. De acordo com Riordan (2019) e Bendiek e Ketteman (2021), a soberania do Estado e as normas e princípios internacionais que dela decorrem, aplicam-se à conduta destes Estados em atividades relacionadas às tecnologias da informação, às comunicações e à sua legislação relativamente às infraestruturas de cada território, os processos intergovernamentais entre Estados explicitam a necessidade de se estabelecer uma agenda de estratégia internacional para a utilização do Ciberespaço como já foi verificado ao longo desta dissertação e passam a influenciar, também, nas práticas diplomáticas contemporâneas as suas iniciativas e realizações e é precisamente neste sentido que a Ciberdiplomacia vem atender aos anseios da comunidade internacional, pois procura integrar uma configuração de normas e processos legais que se imponham de forma relevante na contenção de ciberameaças externas (Bendiek e Ketteman, 2021), uma vez que serve como um complemento da Diplomacia que já conhecemos, no que toca nomeadamente ao modelo de política atual e futura das Relações Internacionais tendo em consideração princípios como a liberdade, a inovação, o crescimento económico, os diferentes usos militares, a Cibersegurança e a governança da Internet proporcionando o desenvolvimento de respostas diplomáticas às ciberameaças que conduzirá a Diplomacia convencional para o desenvolvimento de novas competência para enfrentar os desafios que dificultam uma resposta comum às possíveis formas de guerra no Ciberespaço e aos crimes virtuais, minimizando conflitos e proporcionando formas de compartilhar recursos, tecnologias e canais para empreender esforços na construção de colisões estatais

e privadas, de acordo com o direito internacional, de maneira a assegurar a estabilidade global nestas "ciber" questões.

O envolvimento da Diplomacia com o Ciberespaço na história tem sido amplamente limitado ao uso de tecnologias digitais. Barrinha e Renard (2017), definem a Ciberdiplomacia como um "Universo paralelo" à Diplomacia convencional, mas que atua no Ciberespaço. Trata-se do uso de recursos diplomáticos para garantir os interesses do Estado na realidade digital, e esta abordagem ciberdiplomática torna-se fulcral, uma vez que em prol de manter a ordem no Ciberespaço se torna necessário um fator humano para intervir pois o processo da Diplomacia não se trata apenas de relações entre Estados, e deve levar em consideraçãorelações e diálogos mais amplos, que envolvam entidades como organizações regionais e internacionais, empresas multinacionais, atores subnacionais, redes de defesa e indivíduos influentes, conforme mencionado pelo ex-embaixador britânico Fletcher (2016), em relação aoúltimo grupo, empresários como o presidente do Google, Eric Schmidt, têm um poder de atração difícil de igualar para qualquer representante do Estado, são, do seu ponto de vista, novos imperadores.

A Diplomacia também se estendeu progressivamente a novas áreas de política ao longo dos anos, entrando em territórios políticos desconhecidos, como negociações climáticas ou, ultimamente, questões do Ciberespaço. A Ciberdiplomacia pode ser definida como a Diplomacia no domínio do Ciberespaço ou, por outras palavras, o uso de ferramentas diplomáticas e o desempenho de funções no mesmo âmbito (Diplomacia) de forma a proteger interesses nacionais de uma perspetiva Ciberespacial e esses interesses são geralmente identificados no Ciberespaço nacional ou nas estratégias de Cibersegurança, que geralmente incluem referências à agenda diplomática (Barrinha e Carrapiço, 2017). As questões predominantes na agenda da Ciberdiplomacia incluem Cibersegurança, ciberameaças, construção de confiança, liberdade e governança da Internet. Riordan (2019), menciona cinco abordagens técnicas da Diplomacia para o Ciberespaço:

A primeira abordagem trata-se de uma análise de ciberameaças, na qual o autor afirma que as abordagens técnicas se podem focar no ataque em si, nas tecnologias utilizadas para esse fim e no caminho percorrido para chegar ao ataque em si, onde por sua vez, a Ciberdiplomacia, poderá ser capaz de analisar o fator humano, tendo como foco a vítima

ou suposto autor do ataque.

Uma segunda abordagem surge no sentido em que a Ciberdiplomacia pode ser útil é melhorando estratégias para minimizar ataques, ou seja, esta estratégia pode ser útil em situações em que um cibercriminoso é identificado, pois consiste em enfraquecer psicologicamente o autor do crime, desencorajando-o de atacar.

O terceiro é rotulado por Riordan (2019) como estratégias diplomáticas para melhorar a colaboração entre governos e empresas: no imaginário dos cidadãos, esta colaboração é dada como certa. Na prática, essa relação não é tão verdadeira. O autor defende que uma abordagem diplomática pode ser capaz de construir redes de confiança entre as partes, e assim sendo a coordenação pode ser aprimorada originando uma situação *win- win* para ambas as partes.

A quarta abordagem consiste em colocar a Diplomacia pública em prática. A ideia é reforçar o apoio público. Dentro da sociedade, a Cibersegurança é uma área muito debatida e a opinião pública costuma criticar empresas por falhas na segurança, diplomatas podem promover o diálogo através das redes sociais ou mesmo através de métodos convencionais.

A quinta e última abordagem diplomática proposta pelo autor consiste em socializar a cadeia de abastecimento, isto é, a criação de padrões de atitudes e abordagens comuns para o mundo da Cibersegurança.

Em suma, a natureza empática de um diplomata, juntamente com a sua capacidade de socialização com o público, formas de Diplomacia, campanhas de comunicação estratégica, e outras estratégias semelhantes às acima mencionadas, compõem a base do que a Ciberdiplomacia pode fazer quando o Ciberespaço se encontra sobre ameaça.
A Ciberdiplomacia segundo Barrinha e Renard (2017) é portanto, de uma forma geral conduzida maioritariamente por diplomatas, de forma bilateral (exemplo: diálogos EUA-China), ou multilateral (exemplo: Fóruns da ONU). Para além da missão Diplomática mais tradicional, também é feita a interação Diplomatas/atores não estatais tais como empresários de tecnologia ou organizaçõesda sociedade civil e embora isso defina um alcance bastante amplo de atividades, permite-nos situar firmemente a Ciberdiplomacia como uma instituição da sociedade internacional, mesmo quando interagindo com atores

da sociedade mundial.

A questão da Ciberdiplomacia na UE tem um impacto bastante positivo pois a UE, sendo uma instituição com um sistema global de gestão de crises que promove a estabilidade internacional trabalhando não só dentro como fora das suas fronteiras e que trabalha de forma conjunta para zelar pela proteção dos cidadãos encontra-se dependente desta ação conjunta de todos os seus Estados Membros para alcançar sucesso nesta área, pois não seria possível alcançar tão bons resultados agindo através de ações isoladas dos Estados Membros, assim e respeitando o Comunicado da Comissão Europeia para a estratégia de segurança (2020) é fundamental trabalhar em conjunto para tirar proveito dos pontos fortes da UE e assim fazer a diferença, pois uma vez que a responsabilidade pela segurança de cada país parte dele mesmo, não deixa de ser evidente que no âmbito da Ciberdiplomacia, responder de forma integrada e multidisciplinar ajuda os seus intervenientes nos domínios da segurança e do Ciberespaço.

## 4.2 A influência das redes sociais na Ciberdiplomacia

No decorrer dos últimos anos, temos assistido verificado a evolução cada vez mais complexa da Diplomacia, que se destaca pela utilização cada vez mais marcada das TIC e das plataformas digitais e pela evolução do envolvimento das entidades não estatais no Ciberespaço, nomeadamente no campo das redes sociais.

Fisher (2013) defende que as redes sociais vieram permitir o aparecimento o aparecimento de uma nova sociedade global em rede com mudanças importantíssimas na ordem internacional, que se tem vindo a manifestar sobretudo através de atos de mobilização no Ciberespaço, e as plataformas digitais permitem uma ascensão da população e da opinião da sociedade, no sentido em que hoje em dias, estas plataformas permitem dar voz a qualquer cidadão, de qualquer parte do mundo e relativamente a qualquer temática e neste âmbito, as redes sociais apresentam um papel fundamental.

Em primeiro lugar, tornam-se numa ferramenta legítima de mobilização coletiva, por poder exercer pressão sobre o sistema internacional de tomada de decisão e influência, apresentam um impacto real e direto sobre o sistema internacional e por isso, a comunidade internacional exige cada vez mais participantes político-diplomáticos, que requerem novos motivos/soluções que justifiquem os atos dos seus representantes. Nesta

nova situação internacional, a presença ativa de pessoal político e diplomático nas redes sociais não é mais apenas uma questão de escolha, mas uma questão real de necessidades políticas, pois os governos não devem apenas enfrentar as expectativas sociais que vão surgindo a nível nacional, mas devem manter uma competição saudável com outros concorrentes a nível internacional para obter uma certa prioridade estratégica e neste âmbito a Ciberdiplomacia constitui-se como uma politica externa fundamental num mundo em que as entidades governamentais e não governamentais competem entre si quer por influência, quer por poder num mesmo espaço virtual, espaço esse que detém a atenção de um vasto número de utilizadores que acedem à internet através de diversos dispositivos, e quando utilizada de forma correta, a Ciberdiplomacia é um complemento oportuno de persuasão para a Diplomacia tradicional, podendo ajudar determinado país a expandir os seus objetivos de política externa ao nível internacional, influenciando um maior número de pessoas.

De acordo com Fisher (2013), as redes sociais oferecem uma panóplia de vantagens e oportunidades para alcançar cidadãos de todo o mundo em tempo real, oferecem espaços para interagir, influenciar e consequentemente promover objetivos diplomáticos, tudo isto a um baixo custo, tornando as novas tecnologias e o Ciberespaço, um lugar atraente para muitas embaixadas.

Estas plataformas permitem o uso de conteúdos mais dinâmicos ques e tornam mais atrativos sobretudo para a camada mais jovem da população, tais como links, fotografias e vídeos, e sendo as novas tecnologias instrumentos particularmente úteis no ramo da Diplomacia nomeadamente em questões de processamento de dados e informações, nas atividades consulares e na comunicação de matérias e assuntos importantes, as práticas internacionais têm vindo a demonstrar que o correto e competente uso de ferramentas ciberdiplomáticas pode ser feito a baixo custo, alcançando grandes resultados.

Obviamente que a Ciberdiplomacia funciona como um complemento da Diplomacia tradicional e não como uma possível substituta, até porque o trabalho desenvolvido em todo o mundo por parte dos Ministérios das Relações Externas, continua a ser administrado pelos processos normais da Diplomacia, no entanto a Ciberdiplomacia quando administrada com habilidade, pode fortalecer o trabalho do Estado nas Relações Internacionais e nas políticas externas de uma forma mais rápida, económica e abrangente, o que não significa que a Ciberdiplomacia não tenha as suas falhas.

De acordo com Solomon (2000) ineficiência e perigo são duas das críticas apontadas à utilização do Ciberespaço, em especial das redes sociais para fins políticos e diplomáticos. Solomon (2000), reconhece que informações relativas a crises internacionais passaram a ser transmitidas em tempo real, e que o roubo de dados e informações confidenciais, os ciberataques e o anonimato proporcionado pela internet são riscos reais. Um exemplo de roubo de informação foi o episódio do wikileaks, quando em 2010 foram publicadas cerca de 250.000 correspondências diplomáticas enviadas entre missões dos EUA e o Departamento de Estado em Washington. A utilização das redes sociais e dos recursos tecnológico por parte de diplomatas em todo o mundo, permitiu uma abertura da comunicação entre os legisladores e os cidadãos.

Alves (2021) defende que ferramentas como o Facebook e o Twitter, proporcionam às missões diplomáticas acesso direto aos cidadãos, permitindo alcançar os objetivos diplomáticos pretendidos e esta onda de utilização das redes sociais por parte de políticos e diplomatas coloca de lado várias normas e formalidades protocolares, uma vez que vários aspetos são ignorados para transmitir a ideia de maior proximidade com o público alvo. As abreviações ganhamterreno e o uso de *emojis* entra no dicionário político-diplomático, o que pode ser encarado por muitos como facilidade na comunicação, é encarado por outros como perdade prestígio.

Os atores internacionais tendem cada vez mais a aderir às novas modas que vão surgindo através das redes sociais (Alves, 2021), como é o caso das "*selfies*" e dos vídeos da rede social *tik tok* que transmitem à população um sentimento de proximidade entre as personalidades políticas e a sociedade. Se antigamente, as redes sociais eram consideradas uma obsessão fútil, hoje em dia pelo contrário elas são encaradas como ferramentas com bastante potencial para o desenvolvimento de movimentos sociais e relações diplomáticas em todo o mundo já que a revolução das TICs resultou no controlo da forma como a informação flui em todos os lugares, tornando a disseminação da informação rápida e ampla, permitindo que as pessoas façam os seus próprios julgamentos, expressem as suas preocupações e sentimentos, e até mesmo influenciar políticos e legisladores de todo o mundo e vice versa.

Consequentemente, a forma como os governos interagem é mais rápida e alcança mais cidadãos em quase todas as partes do mundo, isto é, se por um lado, as redes sociais,

transmitem aos países mais informações para resolver os problemas sociais, por exemplo, pessoas em áreas de conflito tendem a usar as redes sociais para angariar apoio, organizar protestos, comunicar, e informar o mundo dos eventos a decorrer nos seus países, especialmente países que se encontram sujeitos a censura e apagões dos mídia, por outro lado, uma série de riscos são associados à utilização das redes sociais como ferramenta ciberdiplomática, fator que parece ser ofuscado pelos benefícios das mesmas (Gordijn, 2020).

A Ciberdiplomacia pode auxiliar em grande escala a projeção das posições de política externa de um estado para um público internacional, assumindo diversas formas e tamanhos, e uma vez que não se limita a barreiras físicas, tendo em conta que toda a sua ação se desenvolve no Ciberespaço, presidentes, primeiros-ministros, advogados, cientistas, diplomatas, organizações governamentais e não governamentais, embaixadores, entre outros exemplificam a diversidade de potenciais atores diplomáticos, mas também a coerênciado esforço para aumentar o poder e influência através de parcerias e estratégias inovadoras, em vez de atos de força unilaterais (Hutchings e Suri, 2015).

A Era da globalização é caracterizada por um aumento e intensificação das interações políticas, económicas e culturais além das fronteiras territoriais, atualmente a política internacional conta com uma vasta gama de atores internacionais unidos na "rede" destes fenómenos e as redes sociais oferecem um mundo de possibilidades (Alves, 2021), como entrar em contato com outras pessoas de outros países e culturas, bem como continuar a manter o contato por meio da troca de experiências e conhecimentos e ainda dinamizar movimentos culturais e políticos por meio do contato com os utilizadores. No entanto, a sua utilização acarreta uma série de riscos derivados do seu uso indevido ou irresponsável com consequências negativas, pois o que pode ser considerado para muitos uma fonte de oportunidades, pode conduzir-nos a uma série de situações menos favoráveis derivadas do seu uso indevido e embora o uso das redes sociais para fins políticos tenha sido questionado e até criticado justamente pelo peso ideológico que carrega, isso não impediu o reconhecimento do poder que gera ruídos e rumores que a própria rede possui, potencial que pode ser aproveitado para fins de comunicação persuasiva. Conforme Gordijn (2020) basta um único comentário dentro da rede para

mudar a situação de certos fenómenos sociais ou mesmo causar conflitos entre os Estados que haviam resolvido as suas diferenças, como mencionado anteriormente o que torna a ação de postar algo na internet onde tudo se move em tempo real num grande impacto nas relações diplomáticas, exemplo disso foi o problema criado pelo embaixador britânico no Chile, (Vergara, 2012) Jon Benjamin, após postar na sua conta no Twitter uma mensagem sobre a disputa entre argentinos e ingleses pelas Malvinas. Nas palavras do embaixador britânico relativamente às ilhas, questionava quais as ilhas que foram tiradas de quem e qual a razão, e este comentário causou um escândalo nas redes sociais, e foi um assunto central entre os utilizadores do Ciberespaço, após este evento o embaixador não teve escolha a não ser excluí-lo da sua conta e oferecer um pedido de desculpas ao país ofendido, garantindo que ele não pretendia ofender ninguém.

O uso de redes sociais para fins de propaganda tem grandes consequências nos países onde ocorre, por exemplo, o ativista bielorrusso Evgeny Morozov argumenta que ter transformado as redes sociais em canais de comunicação atingiu regimes autoritários como Rússia, Cuba, China, entre outros que o fizeram.

Outro dos riscos aos quais os Estados estão expostos por meio das redes sociais é a ciberespionagem diplomática ou governamental, cujo objetivo é o roubo de informações confidenciais, códigos de acesso a sistemas informáticos secretos e dados de dispositivos móveis. A grande vantagem ou desvantagem de todas essas ferramentas é que são públicas e gratuitas, assim, todos podemos ter os nossos próprios canais de comunicação, o que gerou uma grande enxurrada de informações, a grande maioria ociosa e é por isso que os governos ou qualquer organização devem ter clareza sobre o objetivo que desejam alcançar ao usar essas ferramentas. No que se refere à publicação de informações privadas, pode ameaçar a segurança nacional, pois a exposição de documentos secretos ou importantes acarreta uma série de riscos por estarem expostos aos olhos de milhões de usuários que podem utilizá-los indevidamente e importa referir que tais informações prejudicam a imagem de um governo ou uma personalidade política, porque o prestígio é a base das relações internacionais e com o uso indevido das redes sociais torna-se frágil, porque sem prestígio, sem reputação internacional, um país perde as suas armas para interagir com a comunidade internacional.

## 4.3- Ciberdiplomacia como ferramenta política de gestão e prevenção de conflitos na UE

A tendência das nações se tornarem inteligentes traz consigo a preocupação das autoridades para um modelo de conflito em que as suas capacidades de proteção e necessidades de múltiplos domínios atuam sobre as suas infraestruturas de informações críticas e neste âmbito a Ciberdiplomacia vem atender aos anseios da comunidade internacional e visa integrar e convergir uma configuração de normas e processos legais que se imponha de forma relevante na contenção de ciberameaças externas.

A soberania do Estado e as normas e princípios internacionais que dela decorrem aplicam-se à conduta destes em atividades relacionadas às TIC e à sua jurisdição sobre as infraestruturas nos seus territórios, aliás, os processos intergovernamentais entre Estados explicitam a necessidade de se estabelecer uma agenda de estratégia internacional para utilização do Ciberespaço (Manor, 2017) e passam a influenciar, também, nas práticas diplomáticas contemporâneas as suas iniciativas e realizações. Estas ações centram-se, principalmente, em questões ligadas ao domínio do poder do Ciberespaço, à atribuição de ciberataques e identificação de vulnerabilidades da Internet ao instrumento diplomático mais poderoso a ser adotado para respondê-las: o uso de cibersanções.

A Ciberdiplomacia complementa a Diplomacia tradicional (Gilboa, 2016) no modelo político atual e futuro das relações internacionais levando em consideração a liberdade, a inovação, o crescimento económico, os diferentes usos militares, a Cibersegurança e a governança da Internet e o desenvolvimento de respostas diplomáticas às ciberameaças e de certo modo, conduz a Diplomacia convencional para o desenvolvimento de novas competências para enfrentar os desafios que dificultam uma resposta comum às possíveis formas de guerra eletrónica e aos cibercrimes, minimizando conflitos e oferecendo formas de partilha de recursos, tecnologias e canais para empreender esforços na construção de coligações estatais e privadas, de acordo com o direito internacional e de maneira a assegurar a estabilidade global nestas questões do Ciberespaço.

Embora seja um tema novo, a Ciberdiplomacia já avançou a passos largos em todo o mundo na tentativa de definir e sintetizar os esforços constantemente desenvolvidos para resolver um novo tipo de conflito, nomeadamente os que decorrem no Ciberespaço. O papel principal da Diplomacia é gerar vantagem comum por meio do diálogo, portanto, o papel principal da Ciberdiplomacia é gerar vantagem através do diálogo sobre questões de Cibersegurança, mais concretamente, a Ciberdiplomacia usa ferramentas diplomáticas para resolver os problemas que surgem no Ciberespaço.

A última década viu as tecnologias emergentes impactarem os sistemas económicos nacionais no Ciberespaço, o que mudou a agenda diplomática (Bendiek, 2018), com as ciberameaças no seu auge e muitos governos com o reconhecimento de que a Ciberdiplomacia constitui uma mais valia, observa-se uma confusão de terminologia e uma falta de legislação comum ao abordar o tema da Ciberdiplomacia, uma vez que o termo acarreta não só o uso de ferramentas diplomáticas e pensamentos diplomáticos para resolver os problemas do Ciberespaço, mas também o uso de ferramentas digitais para promover agendas diplomáticas mais amplas e o uso de técnicas e mentalidades diplomáticas para analisar e gerir os problemas do Ciberespaço.

O Ciberespaço fornece ferramentas digitais para uma implementação mais eficaz das estratégias diplomáticas, gerando ao mesmo tempo toda uma gama de medidas a nível de governo e outras questões que podem beneficiar das técnicas e da mentalidade do diplomata. Para sustentar questões de segurança de computadores, não basta dirigir-se exclusivamente a equipas técnicas, é o que o ciber-diplomata (Painter, 2018).

De acordo com Bendiek (2018), o desenvolvimento de estratégias diplomáticas mais amplas e voltadas para o futuro pode aprimorar a Cibersegurança, promovendo a colaboração entre governos, empresas e outrosintervenientes importantes e uma vez que a Cibersegurança representa uma prioridade para a política externa de muitosgovernos, há exemplos que podem ilustrar claramente a importância da Diplomacia no contexto geopolítico real no caso Europeu, já que os primeiros atos de Ciberdiplomacia da UE remontam ao início da década de 1990, quando a Comissão Europeia participou em debates internacionais sobre a governança da Internet, seguidos da criação da Corporação da Internet para Atribuição de Nomes e Números (ICANN), no entanto, a estratégia de

Cibersegurança da UE de 2013 representou um marco no desenvolvimento da Ciberdiplomacia da UE, definindo a promoção de uma "política coerente do Ciberespaço internacional" como uma das cinco prioridades principais (Comissão do Alto Representante Europeu, 2013) e declarando que a UE tem como objetivo impulsionar a internet como lugar livre e aberto, promovendo medidas para desenvolver normas aplicáveis ao Ciberespaço, participando de forma ativa juntamente com a comunidade internacional para aumentar a Cibersegurança. (Comissão do Alto Representante Europeu, 2013).

A visão da Ciberdiplomacia da UE baseou-se na identificação de cinco prioridades fundamentais de acordo com o Conselho da UE (2015): promover e proteger os Direitos Humanos no Ciberespaço, implementar normas de comportamento e aplicar o Direito Internacional, a questão da governação da Internet, reforçar a competitividade e prosperidade, bem como capacitar e desenvolver.

Uma sexta prioridade refere-se à Ciberdiplomacia, não tanto aos seus objetivos, mas mais aos seus canais, diz respeito ao envolvimento estratégico com parceiros-chave e organizações internacionais (Conselho da UE, 2015). Esta abordagem pode ser expressa em termos leigos como uma intenção de aprofundar os relacionamentos com uma série de atores importantes do Ciberespaço, em linha com o seu interesse crescente por questões alusivas ao Ciberespaço e os esforços mais amplos para se envolver estrategicamente a nível bilateral com uma série de parceiros.

Relativamente à Ciberdiplomacia, a abordagem da UE desenvolveu-se refletindo uma tendência global e o desenvolvimento da UE como ator diplomático, ainda assim, as questões do Ciberespaço ainda não são a parte mais visível dos esforços diplomáticos globais da EU (Bendiek, 2018), enquanto a maioria dos esforços da UE se concentra na necessidade de aumentar as capacidades europeias e coordenar mais ações, no entanto

importa referir as conclusões do Conselho Europeu relativas ao quadro para uma resposta una da UE na vertente Diplomática contra atividades cibermaliciosas (caixa de ferramentas de Ciberdiplomacia) adotado em junho de 2017 e que visa fornecer uma resposta coletiva da UE a atividades maliciosas através da implementação de medidas diplomáticas no âmbito da PESC que podem ser utilizadas contra operações maliciosas dirigidas contra Estados Membros no Ciberespaço, no entanto ainda não é totalmente

claro que tipo de medidas este conjunto de ferramentas dispõe (Beláz, 2019), mas tratam-se essencialmente de medidas "restritivas" que procuram responder de forma proporcional ao impacto da atividade no Ciberespaço. Importa referir que juntamente com outros esforços, a caixa de ferramentas sublinha a importância dos Estados Membros da UE unificarem a sua resposta diplomática contra as ciberatividades maliciosas (Bendiek, 2018), sendo os esforços diplomáticos comuns vistos como uma forma de reforçar a segurança dos países europeus, claro que as reações aos desenvolvimentos nas tecnologias de comunicação e as interpretações destas implicações para a Diplomacia geralmente passam por várias fases partindo de uma mistura de ceticismo e exagero à aceitação gradual e integração dentro das organizações e para além disso, a maioria dos Ministérios das Relações Exteriores não estão ainda totalmente integrados no Ciberespaço e neste novo modelo de vida digital, no entanto sabemos que os diplomatas necessitarão de estar sempre um passo à frente e de desenvolver as suas capacidades de reinvenção, uma vez que o Ciberespaço e as inovações tecnológicas são lugares que se encontram em constante progresso e evolução.

Muito do que agora é considerado revolucionário logo será visto como comum ou desatualizado e a lacuna entre os governos que não investem na compreensão do impacto da Ciberdiplomacia e aqueles que o fazem será notória. Em suma, podemos afirmar que enquanto principal questão desta Dissertação, a Ciberdiplomacia se constitui como um meio para atingir os fins pretendidos, neste caso, a prevenção e gestão de conflitos na UE, tendo como base as boas práticas governamentais, e segundo Alves (2021), a Ciberdiplomacia pretende aliar uma dinâmica politico-democrática com uma técnica de gestão mais voltada para as ferramentas proporcionadas pelas TIC de modo a garantir uma gestão legitima e eficaz da Ciberdiplomacia perante a comunidade.

Bendiek e Kettemann (2021) defendem que um mundo que segue a mesma linha de inovação precisa de regras comuns e de uma estrutura legal vinculativa para que os mercados comuns possam desenvolver-se e o dilema da segurança possa ser resolvido, se os Estados membros da UE aplicarem uma Ciberdiplomacia conjunta que seja guiada pela máxima da "abertura estratégica" nas suas dimensões institucionais, democráticas e económicas, eles podem garantir que a era do pós-guerra não se tornará na era da pré-guerra digital. A abertura estratégica é fundamental para a manutenção do mercado interno, a fim de efetivamente contrariar os pensamentos de soberania territorial, mesmo

na era digital e neste sentido a autoafirmação no Ciberespaço por parte da UE manifesta-se na redução das dependências, na promoção da capacitação dos direitos civis, na responsabilização das plataformas e no aumento da competitividade da economia europeia. Com esta aspiração em mente, a Ciberdiplomacia da UE deve, segundo Bendiek e Kettemann (2021), em primeiro lugar, ajudar os cidadãos a manter a autodeterminação informativa sobre os seus dados pessoais e em segundo lugar, a Ciberdiplomacia, ao serviço da soberania digital da UE, está ligada à capacidade estratégica de ação e pressupõe que a União também possa fazer valer as suas ideias no âmbito da proteção de dados e segurança a nível internacional. Terceiramente, uma "ressoberanização" europeia na Ciberdiplomacia que é necessária e que significa perceber que um grau mínimo de domínio ou controle da UE sobre os recursos tecnológicos necessários é o que torna a soberania digital possível.

Em quarto lugar, isso inclui garantir que as leis europeias sejam aplicadas ao Ciberespaço e executadas pelos tribunais europeus.

Em quinto lugar, no espírito de reciprocidade e competitividade, seria lógico harmonizar a legislação de segurança de TIC e as regras de licitação e licenciamento a nível da UE (Bendiek e Kettemann, 2021).

Os objetivos referidos acima são atendidos pelo planeamento dos atos jurídicos e estratégias da UE sobre dados, mercados, serviços e algoritmos na Europa e, mais recentemente, sobre a questão da Cibersegurança.

Conforme os avanços da UE, devem avançar também os Estados Membros que devem estar preparados para atualizar a narrativa da Europa como uma força para a paz na Era digital com recurso às politicas e estratégias de segurança e defesa mais robustas e coordenadas e honrando a sua orientação estratégica e ancoragem institucional em Ciberdiplomacia na UE, uma vez que as decisões da maioria qualificada são certamente necessárias para poder responder com medidas restritivas no caso de ciberataques graves.

Bendiek e Kettemann (2021) defendem que a harmonização nem sempre é o caminho para a otimização e que uma abordagem pan-europeia da Cibersegurança significa formalizar o intercâmbio de conhecimentos entre instituições, autoridades de segurança, academia e indústria.

As atividades maliciosas no Ciberespaço minam a ordem internacional baseada em regras,

aumentam o risco de conflito e, consequentemente, representam um risco para a segurança e o bem-estar dos cidadãos (Instituto da União Europeia para Estudos de Segurança, 2019) e por esta razão, a Ciberdiplomacia da UE está empenhada em resolver os litígios internacionais através de meios pacíficos.

Conforme o relatório "Ciberdiplomacia n União Europeia" do Instituto da União Europeia para Estudos de Segurança (2019) para prevenir os efeitos adversos de atividades maliciosas no Ciberespaço, a UE desenvolve um quadro estratégico inclusivo para a prevenção de conflitos através do envolvimento bilateral, regional e de várias partes interessadas, trabalhando para reforçar a ciber-resiliência global, o que reduz a capacidade de criminosos potenciais fazerem mau uso da tecnologia para fins maliciosos e fortalece a capacidade de Estados e sociedades de responder e recuperar de ciberameaças com eficácia. A EU e os seus Membros desempenham um papel ativo na definição da agenda global de Ciberdiplomacia, através da sua presença e ações em todo o mundo, a União Europeia é líder global no reforço e proteção da natureza livre, aberta, segura e pacífica do Ciberespaço (Instituto da União Europeia para Estudos de Segurança, 2019).

## 4.4- Vantagens e Desafios da Ciberdiplomacia

As vantagens da Ciberdiplomacia como extensão da Diplomacia pública são imensas. Primeiramente e de acordo com Alves (2021), o facto de não existirem barreiras físicas no Ciberespaço permite alcançar lugares que até então eram impensáveis, as informações partilhadas no Ciberespaço rapidamente se espalham pelo globo, quebrando qualquer fronteira em questão de segundos.

> *"Uma página de Facebook pode dar informação útil sobre o funcionamento de uma embaixada; uma conta de Instagram mostra a atividade pública do chefe de missão; uma conta Twitter pode explicar posições políticas assumidas pelo país. Mas o mais interessante é que o mundo digital pode servir para que exista um diálogo que o mundo real não permite: com relações diplomáticas cortadas desde 1980, os EUA não*

> *têm, evidentemente, uma embaixada física em Teerão mas têm uma embaixada virtual que pode ser acedida no site https://ir.usembassy.gov/ e que, em inglês e em persa, explica que "this place is for you, the Iranian People…" (*Alves, 2021, p. 124)

O exemplo referido pelo autor, apenas demonstra que a Ciberdiplomacia consegue chegar mais longe ainda do que a Diplomacia tradicional, uma vez que verificamos que a inexistência de uma representação diplomática física não constitui nenhum constrangimento no diálogo direto e eficaz com a população, de fato esta ferramenta permite alcançar vastas audiências de forma rápida e a um baixo custo, sem recurso a métodos intermediários tradicionais como por exemplo a imprensa. Um ministério necessitará apenas de uma vasta gama de seguidores numa rede social para difundir uma mensagem quase que de forma automática: Resultados de eleições em Portugal serão conhecidas rapidamente por qualquer cidadão que se encontre nos EUA por exemplo, a difusão global existente, prática, acessível, rápida e ilimitada é possível fazer a custo zero, em qualquer lugar e através de qualquer dispositivo inteligente que tenha acesso à internet. Enquanto que uma missão diplomática carece de alguns recursos e possui algumas limitações, os instrumentos ciberdiplomáticos apresentam maior utilidade (Alves, 2021).

A Ciberdiplomacia cria uma certa perceção de proximidade, uma vez que graças à rápida difusão de informações vários atores se mobilizam em prol dos mesmos assuntos, situações e acontecimentos e hoje em dia uma ação diplomática entre por exemplo a Suíça e a Itália não conta apenas com os intervenientes responsáveis pela mesma de ambos os países, mas sim com um conjunto de atores que direta ou indiretamente se encontram relacionados ou simpatizados, a favor ou contra à questão tratada.

A facilidade em comunicar que os atores diplomáticos encontram, tem tanto de benéfico como de desvantajoso, tendo em consideração que aquilo que comunicam atinge milhões de pessoas por todo o mundo e com uma rapidez astronómica, informações erradas, excesso de informação ou a má interpretação do público poderá prejudicar o estado em questão ou o próprio ator, já para não referir que é necessária muita atenção no que diz respeito à compatibilidade das informações com o Regulamento Geral de Proteção de Dados.

> *"(...) a verdade é que a emergência da comunicação digital trouxe associada conceitos como fake-news ou pós-verdade. Se a velocidade de circulação da informação é uma vantagem, essa circulação acelerada é altamente problemática quando alavanca inverdades ou estórias que relevam do estrito domínio da desinformação."* (Alves, 2021, p.124).

Alves (2021), refere a algoritmização da informação como outro desafio, uma vez que as páginas e sites que acedemos vão construindo uma espécie de identidade que o software deteta, assume e gere através da seleção automática das nossas preferências. Este processo impede que vejamos aquilo que realmente queremos e sim aquilo construído para nós com base no algoritmo, o que representa um entrave a quem pretende comunicar e fazer uso da Ciberdiplomacia, uma vez que nem sempre a informação alcançará o publico pretendido. Um exemplo apresentado por Manor (2016) mostra-nos que um simpatizante de uma causa na Palestina muito dificilmente irá consultar publicações do Ministério dos Negócios Estrangeiros Israelita, embora até possa ser um seguidor de ambas as entidades nas redes sociais.

A existência de softwares de automação, os chamados "bots" constitui outra desvantagem para o campo da Ciberdiplomacia uma vez que se tratam de usuários inexistentes ficcionados através destes softwares e que automatizam comentários quer positivos (para falsear as estatísticas em beneficio dos próprios Estados / entidades), quer negativos (para publicar comentários desrespeitosos e que descredibilizem outros Estados / líderes estrangeiros) e posto isto as competências e aptidões digitais podem ser vistas tanto como um ponto forte da Ciberdiplomacia como um ponto fraco e sabendo que hoje em dia existem técnicas para chamar à atenção do público alvo nas redes sociais conseguindo tirar o maior proveito destas ferramentas de difusão, e que não só as imagens partilhadas têm importância como a linguagem utilizada, quem dominar estas competências poderá usar isso a seu favor no que toca à aplicação da Ciberdiplomacia, quem por seu lado não domina esta vertente poderá arruinar a mensagem que está a tentar transmitir. O Famoso caso descrito por Alves (2021), do ex Ministro dos Negócios Estrangeiros Sueco, Carl Bildt, postou no seu twitter em 2012 um tweet que ironizava um jantar para falar acerca da problemática da fome no mundo, esta postagem não caiu nas boas graças dos

utilizadores do Ciberespaço e a sua mensagem não só não teve o impacto desejado como teve uma conotação bastante negativa.

## 4.5- Eficácia da Ciberdiplomacia

Num momento em que se regista uma diminuição da confiança entre os representantes políticos e as pessoas ao redor do mundo , uma vez que no campo digital alguns atores têm maior impacto na sociedade e que a não participação do país neste campo de influência digital terá um impacto devastador na sua legitimidade política e diplomática, a prática diplomática é portanto, obrigada a reavaliar os seus procedimentos e adotar uma postura significativamente mais descentralizada, horizontal, inclusiva, pluralista e participativa que vá corresponder a todas as mudanças constantes da esfera pública internacional, porém, toda esta dinâmica repentina não equivale a enfraquecer o processo decisório à medida que aumenta o poder da população, nem deve ser considerada como um mal necessário para a sobrevivência, mas como a evolução da época em processo de adaptação. A narrativa da Ciberdiplomacia desenvolveu-se quase exponencialmente a nível internacional e visa dar legitimidade aos órgãos de governo e às instituições políticas (Moret e Pawlak, 2017).

Em Dezembro do passado ano de 2020, a União Europeia apresentou-nos a sua nova estratégia em matéria de Cibersegurança com o intuito de fortalecer a soberania tecnológica e digital da Europa. O documento lista projetos de reforma que visam aproximar a questão da Cibersegurança e a UE como um todo.

Surgem novas regras acerca dos dados, mercados, serviços e algoritmos do Ciberespaço notando-se que existe uma necessidade quase que urgente de uma Ciberdiplomacia capaz de unir uma abertura estratégica e preservar o Mercado Único Digital, tendo em consideração que a Ciberdiplomacia da UE ainda apresenta algumas falhas devendo ser aprimorada de modo a tornar-se mais coerente.

Segundo dados do CNCS, em 2019, a UE registrou cerca de 450 ataques em infraestruturas críticas na energia e setores de abastecimento de água, bem como informações e tecnologias de comunicação nos setores de saúde, transportes e finanças, o

que nos mostra as vulnerabilidades das sociedades tecnologicamente interdependentes e que se tornaram particularmente evidentes durante a pandemia de Covid-19, uma vez que vários estudos e registos apontam para um aumento generalizado de ciberataques.

Neste sentido, como é que a Ciberdiplomacia se constitui de fato como uma ferramenta eficaz?

No caso específico europeu, o quadro para respostas diplomáticas conjuntas da UE a ciberatividades maliciosas é posto em prática, embora não seja especificado quais serão exatamente os instrumentos que compõem a caixa de ferramentas diplomáticas da UE, a decisão refere-se a medidas no âmbito da Política Externa e de Segurança Comum e a formulação de medidas restritivas, o que significa que aliada às ferramentas diplomáticas comuns, é possível pensar em sanções políticas e económicas contra qualquer adversário que ataque os Estados membros da UE no Ciberespaço (Beláz, 2019).

Esse tipo de ferramenta de retaliação diplomática pode funcionar como um impedimento, tornando as ciberameaças menos anónimas e livres de risco, ao mesmo tempo que acarreta poucos riscos.

A história recente de ciberincidentes mostra que os cibercriminosos são um grande problema global (Carrapiço e Barrinha 2017), mas que os estados são responsáveis pelo desenvolvimento das armas mais poderosas do Ciberespaço (através da exploração de bots, bugs e softwares). Apenas atores estatais (ou apoiados pelo Estado) têm capacidade financeira e humana suficiente para investir no desenvolvimento das armas do Ciberespaço mais poderosas e infelizmente os esforços para conter o comportamento agressivo dos Estados no Ciberespaço através do desenvolvimento da definição de normas internacionais das Nações Unidas têm vindo a fracassar e isto deve-se à falta de regras comuns de comportamento, os Estados também podem contar com a dissuasão de ciberataques.

Muitos Estados prometem retaliar os ciberataques com ações militares (Reino Unido pré-Brexit ameaçou fazer uso de retaliação aérea contra ciberataques) ou de forma mais pacifica e resiliente fazendo uso da Ciberdiplomacia, iniciativa que se constitui como um desenvolvimento valioso e que deve ser apoiada pelos estados membros da UE, mas que levanta também algumas questões e que segundo Limnéll e Meer (2017) devem ser consideradas e que colocam em risco a sua eficácia.

Em primeiro lugar, um grande problema é que os países da UE diferem nos seus níveis de preparação para as questões do Ciberespaço e isto torna difícil cumprir o princípio da solidariedade operacional (que os Estados Membros estariam realmente dispostos a apoiar-se mutuamente e, em particular, seriam capazes de executar uma resposta diplomática conjunta da UE), em vários Estados Membros da UE é necessário um compromisso político mais forte para melhorar o nível de prontidão no Ciberespaço, caso contrário, a "ciber-solidariedade" enfraquece e a resposta conjunta é mais difícil de realizar.

Em segundo lugar, os meios diplomáticos de resposta são importantes, mas é importante ter em consideração que também existem muitas outras opções de resposta, quem estabelece e formula as políticas precisam considerar toda a vasta gama de respostas à sua disposição, desde uma repreensão diplomática até um ataque militar. Por vezes, a resposta diplomática por si só é eficaz, em casos mais graves nem por isso e aí torna-se necessária outro tipo de intervenção que complemente a primeira e portanto torna-se necessário um quadro abrangente da UE com diferentes formas de resposta que vão além dos instrumentos ciberdiplomáticos, sem deixar de complementar os mesmos.

O terceiro ponto complementa o anterior uma vez que apesar dos Estados Membros da UE concordarem com o conteúdo da "Caixa de ferramentas ciberdiplomáticas", deve haver processos políticos e determinação para implementá-la concretamente quando um Estado Membro é atingido por um ciberataque.

A vontade política conjunta para responder deve ser discutida exaustivamente com antecedência e é bom exercê-la também.

Em quarto lugar, o combate às ameaças híbridas é uma prioridade europeia e o papel das operações no Ciberespaço na guerra híbrida tem vindo a aumentar, no entanto, geralmente não existem operações apenas no Ciberespaço e a guerra híbrida é caracterizada pelo uso personalizado de todos os instrumentos de poder contra as vulnerabilidades dos sistemas do oponente. Portanto, criar ferramentas de resposta ciberdiplomática apenas contra ciberataques acaba por não ser suficiente em determinadas situações (Limnéll e Meer 2017).

Segundo Policarpo (2021), a Ciberdiplomacia apresenta grandes vantagens mas apenas após alcançar algumas melhorias propostas pelo CNCS*, pois muito

provavelmente, haverá simultaneamente outros instrumentos de influência usados e eles devem ser levados em consideração relativamente à resposta e de forma a atingir o sucesso na utilização da caixa de ferramentas ciberdiplomáticas e usufruir da sua eficácia máxima, a UE deve reforçar as suas capacidades para poder atribuir melhor os ataques, melhorar a indústria europeia de Cibersegurança e aumentar a investigação multidisciplinar em matéria de Cibersegurança na Europa. Em suma, a iniciativa da "Caixa de ferramentas ciberdiplomáticas" pode abrir uma nova e importante página na dissuasão europeia no Ciberespaço, mas apenas se for apoiada por um forte compromisso político e se o contexto mais amplo for compreendido. Atualmente com a comunicação digital a assumir este papel de elevada importância nas relações sociais, diminuindo distâncias físicas e permitindo comunicar em tempo real para qualquer parte do mundo e destacando as redes sociais que têm um papel fundamental ao elevar a voz da opinião pública a patamares nunca antes explorados, as entidades político-diplomáticas vêm-se obrigadas a alterar as suas estruturas tradicionais e a adaptarem-se a este jogo de influências digitais. De facto, as entidades político-diplomáticas não têm outra opção senão adaptarem-se e desenvolver estratégias digitais, se pretendem sobreviver neste novo plano comunicativo, ou seja, num sistema internacional em constante interação e interdependência, a adoção da Ciberdiplomacia enquanto instrumento de comunicação com o exterior, não se trata apenas de uma mera opção estatal, mas sim de uma verdadeira questão de necessidade político-diplomática que acompanha a evolução dos tempos. O Ciberespaço e nomeadamente as redes sociais (como já verificámos) vieram assim permitir a junção improvável de duas comunidades aparentemente distintas e distantes: a comunidade político-diplomática por um lado, elitista, reservada e tradicional; e a comunidade civil por outro lado, popular, fortemente interconectada e moderna, e o que se espera da comunidade político-diplomática é precisamente que esta se adapte às regras que regem as redes sociais e que proceda em congruência com as mesmas, não abdicando, porém, das suas especificidades. Neste sentido, a Ciberdiplomacia desafia-se a ela própria elevando a fasquia das expetativas internacionais a um patamar nunca antes explorado, tanto por parte da população como por parte das instâncias decisivas na arena da comunicação político-diplomática.

*****Verificar documento em anexo: B1.

# Considerações finais

Como é possível observar ao longo do século XXI, as alterações ocorridas nas formas de implementação da Diplomacia são mais evidentes, o chamado Soft Power adquiriu maior relevância em relação aos métodos tradicionais de influência ou coerção e tudo isso tem sido consequência de uma série de fatores que foram identificados ao longo desta pesquisa como a interdependência, o fortalecimento da opinião pública, a revolução nos meios de comunicação de massa, o fluxo de ideias e informações e a globalização principalmente através da cultura.

Atualmente é possível afirmar que os Estados reformularam as suas estruturas de política externa e elevaram a Diplomacia a outro patamar, onde o Ciberespaço passou a ser palco de ação direta e efetiva no desenvolvimento de estratégias em conjunto com outros atores internacionais para a solução dos problemas da agenda internacional, promovendo a paz na esfera global, e o desenvolvimento e respetiva implementação de ações de Ciberdiplomacia tem conduzido os Estados, em diversas ocasiões, a uma abordagem e ao diálogo político para preservar a paz no mundo e tratar das questões de segurança no Ciberespaço, constituindo-se como uma ferramenta bastante eficaz e válida da caixa de ferramentas da UE para prevenir o cibercrime e ciberameaças, uma vez que a Ciberdiplomacia sendo a componente paralela da Diplomacia a atuar no Ciberespaço constitui a chave do fator humano para a promoção de um Ciberespaço mais pacífico.

As principais ações realizadas neste sentido variam desde a análise de ciberameaças à minimização dos seus riscos e incrementando a cooperação entre empresas e governos, criando redes e estabelecendo padrões de ação, o que pode ser posto em prática através da consciencialização através da Ciberdiplomacia, relativamente à importância da Cibersegurança, o que nos permite concluir que esta se trata de uma ferramenta muito eficaz para preencher as lacunas que a neutralidade ou a questão da atribuição, inerentes ao Ciberespaço podem deixar derivados da mitigação de conflitos no Ciberespaço.

A maioria dos governos começou a aderir à nova era digital, em que as redes sociais permitiram que as ações diplomáticas no Ciberespaço modificassem os padrões tradicionais da Diplomacia, e tendo em conta que hoje os problemas exigem maior capacidade de resposta frente aos fenômenos de crise, a Ciberdiplomacia e a sua correta aplicação podem contribuir para o entendimento das nações, é necessário destacar que a

Ciberdiplomacia, graças às suas ferramentas eficazes e aos seus múltiplos benefícios, tornou-se um instrumento de primeira ordem para influenciar a realidade internacional, constituindo-se como um fator inovador e altamente eficaz parao pleno exercício da Diplomacia tradicional numa outra dimensão que acaba por estar diretamente ligada ao nosso mundo físico. Não se reflete apenas na reestruturação do papel do diplomata, mas vai além, transformando as suas estruturas internas para uma melhor assimilação da ciência e da tecnologia, inovando com novas diretrizes da Ciberdiplomacia, não só através de ações e missões no Ciberespaço, mas também através das embaixadas e consulados virtuais.

Num contexto em que o desenvolvimento das TIC alterou a forma como comunicamos dando acesso a uma maior liberdade de informação, os Estados implementam principalmente essas tecnologias para o desenvolvimento das suas atividades diplomáticas de uma forma mais eficaz. Portanto, a assimilação tecnológica pela Diplomacia foi necessária e, além disso, começaram a modificar não só o papel do diplomata, mas também as estruturas e locais de trabalho, é aí que a Ciberdiplomacia ganha outro sentido ao criar embaixadas e consulados virtuais que permitem em tempo real interagir com os seus cidadãos e alvos em qualquer lugar sobretudo em locais onde embaixadas e consulados físicos representa um custo maior comparativamente com os virtuais.

A maioria dos países desenvolvidos analisam a iniciativa de substituir representações físicas por virtuais, principalmente em países onde há muitos conflitos ou são áreas de alto risco para representantes diplomáticos.

Embora possa parecer algo muito rebuscado, não está longe da realidade que em termos económicos significa uma opção viável para a maioria dos países que não possuem recursos suficientes para manter representações físicas noutras nações.

Por outro lado, a utilização das redes sociais e sites institucionais como meios importantes para oferecer de forma mais eficaz alguns serviços diplomáticos e consulares desenvolveram dois tipos de relações na representação do Estado: quem é embaixador-embaixador e quem é embaixador-cidadão, quem tem mostrado grande interesse em eventos internacionais e tem se envolvido para ter maior influência nas decisões dos países em situações de conjuntura, estabelecendo o padrão para um melhor fluxo de comunicação através dessas ferramentas que a internet nos oferece.

Quanto aos benefícios dos sites do Estado para a comunidade académica do mundo, é muito útil devido à grande quantidade de dados e documentos substancialmente importantes que são digitalizados a respeito daquele país como constituições, notícias, relatórios de resoluções, tratados e a posição do país sobre um determinado tema a ser debatido a nível internacional, de modo a que a criação de uma embaixada virtual otimizaria o atendimento aos cidadãos nacionais e estrangeiros.

Embora a maioria dos países possuam páginas web, estas servem apenas como consulta, não prestando qualquer tipo de serviço que facilite a agilização dos procedimentos aos cidadãos e perante o risco que representa a era digital, é necessário articular todas as instituições de segurança dos países que permitem e garantem a proteção necessária para evitar que roubos de informações ou dados importantes caiam nas mãos de criminosos que procuram destabilizar a ordem nos países, e não podemos descredibilizar e ignorar o crescente uso da tecnologia nas estruturas governamentais de países que estão a transformar o papel das instituições a nível internacional, e os próprios Estados não ficam de fora dessas inovações que visam contribuir para o aprimoramento e a execução da Ciberdiplomacia do ponto de vista internacional.

Em situações de crise, a Ciberdiplomacia pode ser a chave, especialmente em áreas onde a instabilidade política é uma constante e neste sentido tanto os Estados Membros como os seus aliados têm procurado formas de defender a sua soberania e os seus interesses nacionais e globais no Ciberespaço, sejam estes de índole económica, civil ou militar, e este percurso no Ciberespaço tem influenciado decisões a nível político e estratégico, bem como formas de ataque, defesa e dissuasão contra as ameaças que vão surgindo e uma vez que toda esta inovação das Tecnologias de Informação e Comunicação, acarreta consigo preocupações nomeadamente nas questões de segurança e conflitos, a Ciberdiplomacia torna-se um ator fulcral para dar resposta às questões da comunidade internacional, visando integrar um conjunto de normas e processos que permitam fazer face às ameaças da Era digital e no âmbito desta dissertação que se foca na UE torna-se portanto necessário o reforço de uma agenda estratégica que regule a utilização do Ciberespaço , tendo em consideração que um dos grandes desafios do mesmo passa pela dificuldade de atribuição dos ciberataques , uma vez que o uso de sanções tem constituído uma problemática devido àsdificuldades na sua definição e aplicação, tendo sido aplicadas no presente ano de 2020, as primeiras sanções contra ciberataques. De modo a promover

a segurança do Ciberespaço, e através do desenvolvimento contínuo de respostas diplomáticas a este grande desafio de prevenção e gestão de ciberameaças ideal será potencializar o desenvolvimento de novas estratégias que permitam enfrentar os desafios que dificultamuma resposta unificada dos Estados Membros da União Europeia, que minimize os conflitos e compartilhe novos recursos e estratégias entre países, mantendo sempre comobase o direito internacional, e procurando alcançar a estabilidade global no Ciberespaço.

A criação de plataformas e a formação de pessoal especializado permitirá que a Ciberdiplomacia atue como ferramenta capaz na gestão e prevenção de conflitos na UE, uma vez que através do diálogo é possível apaziguar certas questões e quezílias, bem como estabelecer relações cada vez mais fortes entre os Estados.

A Ciberdiplomacia é apresentada como uma prática essencial para enfrentar os desafios do Ciberespaço e neste âmbito os diplomatas acabam por usufruir dos benefícios que o Ciberespaço tem para oferecer nomeadamente nas áreas do diálogo e interação e a participação e cooperação de todos os atores internacionais será necessária para o desenvolvimento de estratégias que permitam uma resposta imediata a qualquer ciberameaça, ação mais complicada uma vez que nem sempre todos os países e envolvidos se encontram de acordo nas mesmas temáticas e portanto torna-se bastante importante a existência de coordenação entre os centros de segurança dos países, para que a informação flua sem obstáculos e permita detetar estes casos de riscos de Cibersegurança, conseguindo prevenir catástrofes a nível internacional. Como já foi mencionado, a formação de pessoal adequado em matéria digital pode evitar o uso indevido de ciberferramentas que podem gerar conflitos entre dois ou mais países e além disso, a transparência nos processos diplomáticos e governamentais poderá estabelecer os canais de comunicação e confiança com populações remotamente distantes, e não só com elas, mas também com sua própria população.

As principais atividades da Ciberdiplomacia já estão incluídas nas estratégias de política externa dos vários países da UE, na agenda da Diplomacia da UE década de 2020 constatamos que a Ciberdiplomacia tem vindo a colocar em prática as ferramentas clássicas da Diplomacia bilateral e multilateral, já adaptadas ao Ciberespaço. Os desafios das organizações na atualidade estão relacionados com a mudança, adaptação, eficiência e eficácia que transformaram a tradição em inovação e neste tipo de situação a

Ciberdiplomacia mostra-se uma ferramenta bastante capaz na prevenção e gestão de conflitos na UE  uma vez que consegue uma aproximação entre povos e países por meio de relações de cooperação e negociações pacificas, o que de certa forma é uma ótima estratégia no apaziguar de conflitos e na prevenção de diversas situações e a Ciberdiplomacia através destas estratégias para minimizar ataques consegue facilmente enfraquecer psicologicamente um hacker por exemplo, um diplomata pode usar a rede de influência da sua lista de contatos para pressionar o atacante, o hacker pode ser isolado da sua comunidade ou até desencorajado de atacar, o que, em certo sentido, se assemelha a uma dissuasão, mas com uma abordagem menos agressiva, o tal Soft Power referido por Nye (2008). Simultaneamente, este tipo de abordagem diplomática no Ciberespaço pode ser capaz de construir redes de confiança entre as partes e desta forma, a coordenação pode ser reforçada e uma situação *win-win* tanto para as empresas quanto para os Estados em questão.

# Referências Bibliográficas

***Livros e artigos científicos:***


Alves, D (2021), Diplomacia 2.0: riscos e oportunidades num tempo de transição digital, Negócios Estrangeiros N.º 20. MNE, Lisboa.

Azpíroz, M. (2015),. Soft Power and Public Diplomacy: The Case of the European Union in Brazil. Figueroa Press, Los Angeles.

Barrinha, A. Renard, T. (2017), Cyber-diplomacy: the making of an internationalsociety in the digital age, Global Affairs. Routledge, London.

Beláz, A. (2019), The changing role of the EU in cybersecurity. Biztonságtudományi Szemle Safety and Security Sciences Review.

Bendiek, A. (2018), The EU as a force for peace in international cyber diplomacy. Berlin: Stiftung Wissenschaft und Politik, SWP Deutsches Institut für

Bendiek, A; Kettermann, M.(2021), Revisiting the EU Cybersecurity Strategy: ACall for EU Cyber Diplomacy. Berlin: Stiftung Wissenschaft und Politik, SWP Deutsches Institut für InternationalePolitik und Sicherheit, Berlin.
InternationalePolitik und Sicherheit, Berlin.

Bindi, F. (2010), The Foreign Policy of the European Union: Assessing Europe's Role in the World, Brookings Institution Press, Washington.

Brandão, A. (2010), O Tratado de Lisboa e a Security Actorness da UE, Relações Internacionais Nº 25, Instituto Português de Relações Internacionais, Lisboa.

Breene, K. (2016), Who are the cyberwar superpowers?, World Economic Forum disponível em: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/(último acesso em 10.10.2021).

Carrapico, H; Barrinha, A. (2017), The EU as a coherent (cyber)security actor? –JCMS, Volume 55. Number 6.

Carreiras, H et all. (2020), A pandemia covid-19: que impacto nas áreas da segurança e defesa?, Instituto da Defesa Nacional, Lisboa.

Cêlik, P. (2019), Institutional measures for increasing the cyber security for business in the european union, Higher Educational Institution for Applied Studies for Entrepreneurship, Belgrade, Republic of Serbia

waChristen, M; Gordijn, B ; Loi, M; et all. (2020), The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology 21, London.

Christou, G. (2014), The EU's approach to cyber security, University of Warwick, Conventry.

Christou, G. (2016), Cybersecurity in the European Union: Resilience and adaptability in governance policy, Palgrave Macmilian, London.

Delerue, F. (2020), Cyber Operations and International Law, Cambridge University Press, Cambridge.

Dewar, S. (2017), The European Union and Cybersecurity: A Historiography of an Emerging Actor's Response to a Global Security Concern. In: O'Neill, M. Swinton, K. Eds.: Challenges and Critiques of the EU Internal Security Strategy. Cambridge Scholars Publishing, Cambridge.

Duke, S e Ojanen, H. (2006), Bridging Internal and External Security: Lessons from the European Security and Defence Policy, European Integration, Routledge, London.

Fisher, E. (2013) From Cyber Bullying to Cyber Coping: The Misuse of Mobile Technology and Social Media and Their Effects on People's Lives, Business and Economic Research ISSN, Vol.3, London.

Fletcher, T. (2016), Naked diplomacy: Power and statecraft in the digital age, William Collins, London.

Geraldes, S. (2019), A Estratégia de Cibersegurança da União Europeia: Catastrofista, Realista e/ou otimista?, Instituto Universitário de Lisboa, Centro de Estudos Internacionais, Lisboa.

Gibson, W.(1984), Neuromancer, Ace Books, New York.

González, G; Fuster e Jasmontaite, L. (2020), Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology 21, London.

Gilboa, E. (2016) Digital Diplomacy, The Sage handbook of Diplomacy, Sage, Los Angeles.

Hamdouni, Y. (2013), "Internet y La primavera árabe: hacia una nueva percepción del ciberespacio". Paix et Secuite Internationales, Núm.01.

Herrmann, D; Pridhol, H.. (2020), Basic Concepts and Models of Cybersecurity. The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology 21, London.

Howard, F 1993, "Democratizando el ciberespacio", Revista Latino-americana de comunicação, Centro Internacional de Estudos Superiores de Comunicação da América Latina, CIESPAL, Núm. 45.

Hutchings, R; Suri, J. (2015) Foreign Policy Breakthroughs: Cases in Successful Diplomacy, Oxford University Press, Oxford.

Kasper, A; Antonov, A. (2019), Towards Conceptualizing EU Cybersecurity Law. ZEI Discussion Paper C253, Universidade de Bonn, Bonn-Germany.

Kovac, L. (2018) Cyber security policy and strategy in the European Union and NATO, national university of public service, revista academiei forţelor terestre nr. 1 (89), Budapest, hungary

Kozlowski, A. (2018), The European Union Effective System of Sanctions Against Cyberattacks, The Visio Journal, Volume 3, Slovenia.

Kovács, L. (2018), Cyber security policy and strategy in the European Union and NATO, National University of Public Service, Land Forces Academy Review vol 23, n° 1, Hungary.

Kremer, J; Benedickt, M. (2014) Cyberspace and International Relations, Theory, Prospects and Challenges. Springer, University of Bonn, Bonn, Germany.

Lindstrom, G; Tardy, T. (2019), The EU and NATO : The essential partners, European Union Institute for Security Studies, Paris.

Lopez, J. (2020), Ciberdiplomacia y ciberdefensa en la Unión Europea, Thonsom-Aranzadi, Pamplona.

Ludlow, P. (2010), WikiLeaks and Hacktivist Culture, Nation Company L.P, New York.

Manfred, L. (1968), La mecánica de la Diplomacia moderna, Faculdade de Direito da Varsóvia, Varsow.

Manor, I. (2016), What is Digital Diplomacy and how is it is practiced around the World?

- A brief introduction, The Diplomatist Magazine n. 36, Oxford.

Meulen, N; Soesanto, S. (2015) Cybersecurity in the European Union and beyond: exploring the Threats and policy responses, directorate general for internal policies, Policy Department Citizens' Rights and Constitutional Affairs, European Parliament, Brussels.

Mcclellan, S; Jimenes, J; Koutitas, G. ( 2018), Smart cities: Applications,Technologies, Standards, and Driving Factors, Springer, Berlin.

Miller, S. (2020), Freedom of Political Communication,
Propaganda and the Role of Epistemic Institutions in Cyberspace. The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology 21, London.

Moret, E ; Pawlak, P. (2017) ,The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? - European Union Institute for Security Studies (EUISS).

Mueller, M. (2017), Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace, Polity, Cambridge, Malden.

Nicholson, J. (1996), Diplomacy, Institute for the study of Diplomacy.

Nye, J. (2008), Public Diplomacy and Soft Power, SAGE Journals, New York.

Nye, J. (2010), Cyber Power, Belfer Center, Harvard Kennedy School, Cambridge.

Painter, C. (2018) Deterrence in cyberspace, Spare the costs, spoil the bad state actor: Deterrence in cyberspace requires consequences, Australian Strategic Policy Institute, Vol.4, Australia

Pamment, J.(2016), British Public Diplomacy and Soft Power, Diplomatic Influence and the Digital Revolution, Palgrave Mcmillian, London

Pinto, L. (2019), Portugal e três décadas de Política de Segurança e Defesa na União

Europeia. Observare - observatório de relações exteriores, Universidade autónoma de Lisboa, Lisboa.

Potter, E. (2002), Cyber-diplomacy: Managing Foreign Policy in the Twenty-firstCentury, McGill-Queen's Press, Political Science & International Studies: International Affairs/Foreign Policy, Canada.

Reardon, R; Choucri, N. (2012), The Role of Cyberspace in International Relations: A View of the Literature, Department of Political Science, MIT, ISA Annual Convention, San Diego.

Reis, R e Staloch, C. (2015), A mediação das relações sociais nas redes sociais virtuais: do ciberespaço ao ciberterritório, Estudos em Comunicação nº 20, Universidade do Estado de Santa Catarina, Florianópolis.

Riordan, S. (2019), Cyberdiplomacy: Managing Security and Governance Online, Polity Press, Cambridge.

Silva, A.(2004), Arte, interfaces gráficas e espaços virtuais ", *ARS , São Paulo.*

Silva, T; Teixeira, T e Freitas, S. (2015), Ciberespaço: uma nova configuração do ser no mundo, Psicologia em Revista v. 21, n. 1, Belo Horizonte.

Solomon, M. (2000) Icons and Avatars: Cyber-Models and Hyper-Mediated Visual Persuasion, Berry College, Georgia.

Taddeo, M. (2014) The Ethics of Information Warfare, Springer Science & Business Media, Berlin.

Teixeira, N. (2010), A defesa europeia depois do Tratado de Lisboa. Relações Internacionais nº25, Lisboa.

Tikk, E, Kaska, K e Vihul, L. (2010), International Cyber Incidents: Legal Considerations,

Cooperative Cyber Defence Center of Excellence, Tallinn, Estonia

Walker, J; Ludwig, J. (2017),Sharp Power: Rising Authoritarian Influence, International Forum for Democratic Studies, National Endowment for Democracy, Washington.

Wendt, E; Jorge, H. (2013), Crimes Cibernéticos: Ameaças e procedimentos de investigação , 2º Edição, Brasport, Rio de Janeiro.

Werner, M. (2012), Cybersecurity: A Pre-history. Taylor Francis, UK.

***Trabalhos académicos:***

Arrais, H. (2014) A mídia das relações internacionais: aproximações epistemológicas. Graduação no Curso de Relações Internacionais, Universidade de Brasília, Brasília. Disponível em: https://bdm.unb.br/bitstream/10483/7926/1/2014_CesarHenriqueArrais.pdf. Último acesso: 17.06.2020.

Pinto, F. (2019), Enquadramento Técnico-Jurídico da Segurança do Ciberespaço Aplicabilidade na Marinha, Dissertação para obtenção do grau de Mestre em Ciências Militares Navais, na especialidade de Marinha, Escola Naval, Alfeite.

***Webgrafia:***

Ashbrook , C, Política exterior, 2020 - https://www.belfercenter.org/ último acesso: 10.10.2021

Borrel, J. (2020), Sanções contra ciberataques: é tempo de agir! - https://eeas.europa.eu/headquarters/headquarters-homepage/83807/san%C3%A7%C3%B5es-contra-ciberataques-%C3%A9-tempo-de-agir_pt, último acesso: 10.10.2021

Manzano, A; Satow, E. (2012), ¿Qué es la Diplomacia?", Associação de diplomáticos escritores, Revista ADE, disponível em: https://www.protocolo.org/ceremonial/protocolo-diplomatico/que-es-la-diplomacia.html (último acesso em 10.10.2021).

Nye, J. (2004), The Benefits of Soft Power, Harvard Business School, disponível em:

https://hbswk.hbs.edu/archive/the-benefits-of-soft-power (último acesso em 10.10.2021).

Limnell, J ; Meer, S. (2017), Artigo de opinião: EU cyber diplomacy requires more - https://euobserver.com/opinion/138456, último acesso: 10.10.2021

Lobato ,L e Kenkel, K. (2015), A Ciberguerra é Moderna! Uma Investigação sobre a Relação entre Tecnologia e Modernização na Guerra, vol. 37, no 2, Rio de Janeiro, disponível em: https://www.scielo.br/j/cint/a/RQqF3Ztm49nqj4BqKPJGF5J/?lang=pt (último acesso em 10.10.2021).

Rede social Twitter: https://twitter.com/carlbildt (último acesso em 01.09.2021).

Vergara, C. (2012), Polémico tweet de un embajador británico, La Nacion, disponível em: https://www.lanacion.com.ar/politica/polemico-tweet-de-un-embajador-britanico-nid1517641/ (último acesso em 04.10.2021).

***Conferências e fóruns:***

Chris P. (2018) Discurso 30º encontro internacional do CERT em Kuala Lumpur.

Miadzvetskaya, Y. (2020), Restrictive measures: a deterrence tool of the EU Cyber Diplomacy? , Closing the Gap Conference paper, Brussels.

***Documentos oficiais:***

Comunicado da Comissão do Parlamento Europeu, sobre a Estratégia da União Europeia para a Segurança de 24 de Julho de 2020, COM/2020/605, Brussels, EUR-Lex:Direito da EU

Conselho Europeu (2017), G7: Reuniões de Ministros das Relações Exteriores, Statement on the Fight Against Terrorism and Violent Extremism, Taormina, disponível em: https://www.consilium.europa.eu/media/23562/26-g7-statement-fight-against-terrorism-

and-violent-extremism.pdf (último acesso em 02.11.2021).

Conselho Europeu (2019), Ciberataques: Conselho pode agora impor sanções, Comunicado de imprensa, disponível em: https://www.consilium.europa.eu/pt/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/pt (último acesso em 02.11.2021).

Conselho Europeu (2020), Cibersegurança: como combate a UE as ciberameaça, Disponível em: https://www.consilium.europa.eu/pt/policies/cybersecurity/ - último acesso: 15.01.2021

Diretiva SRI 2016/1148 do Parlamento e Conselho Europeu, 6 de Julho de 2016 , , Regulamento ENISA 526/2013 EUR-Lex:Direito da UE

Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")– Disponível em https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf - último acesso: 19.01.2021

Parlamento Europeu – Política externa: Objetivos, Instrumentos e Realizações. Fichas técnicas sobre a União Europeia. Disponível em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_5.1.1.pdf - último acesso: 15.01.2021

Parlamento Europeu – Política Comum de Segurança e Defesa. Fichas técnicas sobre a União Europeia. Disponível em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_5.1.2.pdf - último acesso: 15.01.2021

Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 de abril de 2019 EUR-Lex:Direito da UE

Resolução do Parlamento Europeu, de 21 de janeiro de 2016, sobre a cláusula de defesa mútua (artigo 42.º, n.º 7, TUE) (2015/3034(RSP)) EUR-Lex:Direito da

UE

Serviço Europeu de Ação Externa (2020) - Towards a more secure, global and open cyberspace:the EU presents its new Cybersecurity Strategy, Disponível em: Towards a more secure, global and open cyberspace: the EU presents its new Cybersecurity Strategy - EuropeanExternal Action Service (europa.eu) - último acesso: 19.01.2021

Tratado de Lisboa. JO C 306. 17.12.2007 EUR-Lex:Direito da EU
Tratado de Maastricht. JO C 191. 29.07.1992. EUR-Lex:Direito da UE

União Europeia, (2019), Cyber Diplomacy in the European Union, EU Institute for Security Studies, Office of the European Union, Luxembourg.

# Anexos

# A - Transcrição das entrevistas realizadas

## A.1 – Entrevista com Luís Policarpo - CNCS.

Luís Policarpo, chefe do Departamento da Gestão da Informação Classificada e Criptografia do Centro Nacional de Cibersegurança, realizada via email a 09 de fevereiro de 2021.

**Questão 1:** "Quais são atualmente os principais desafios de Cibersegurança em Portugal?"

**Resposta:** "Considero que os principais desafios da Cibersegurança são e por esta ordem:

1. Iliteracia digital- As pessoas continuam a não apreender os conceitos básicos de ciber higiene
2. Pouco investimento na formação e na atualização dos sistemas e redes por parte das entidades publicas e privadas
3. Pouco envolvimento da liderança das organizações na necessidade em formação das pessoas e na necessidade de investimento. Este investimento não apresenta frutos imediatos dai essa relutância."

**Questão 2:** "Muitos autores e entidades defendem que a Ciberdiplomacia é uma ferramenta com bastante potencial na luta pela preservação da Cibersegurança. Do seu ponto de vista, a Ciberdiplomacia apresenta alguma vantagem no âmbito da Cibersegurança?"

**Resposta:** " A Ciberdiplomacia apresenta alguma vantagem mas considero que sem se atingir o nível de maturidade 3 definido no quadro de referencia de Cibersegurança do CNCS * (que anexo) serve só para "show off".
Nestes 4 anos foi o que vi pelo menos em Portugal."

**Questão 3:** "A Ciberdiplomacia constitui uma das ferramentas ou potenciais ferramentas utilizadas pelo Gabinete Nacional de Segurança nas questões de Cibersegurança e defesa? Se sim, de que forma é feita a aplicação da mesma?"

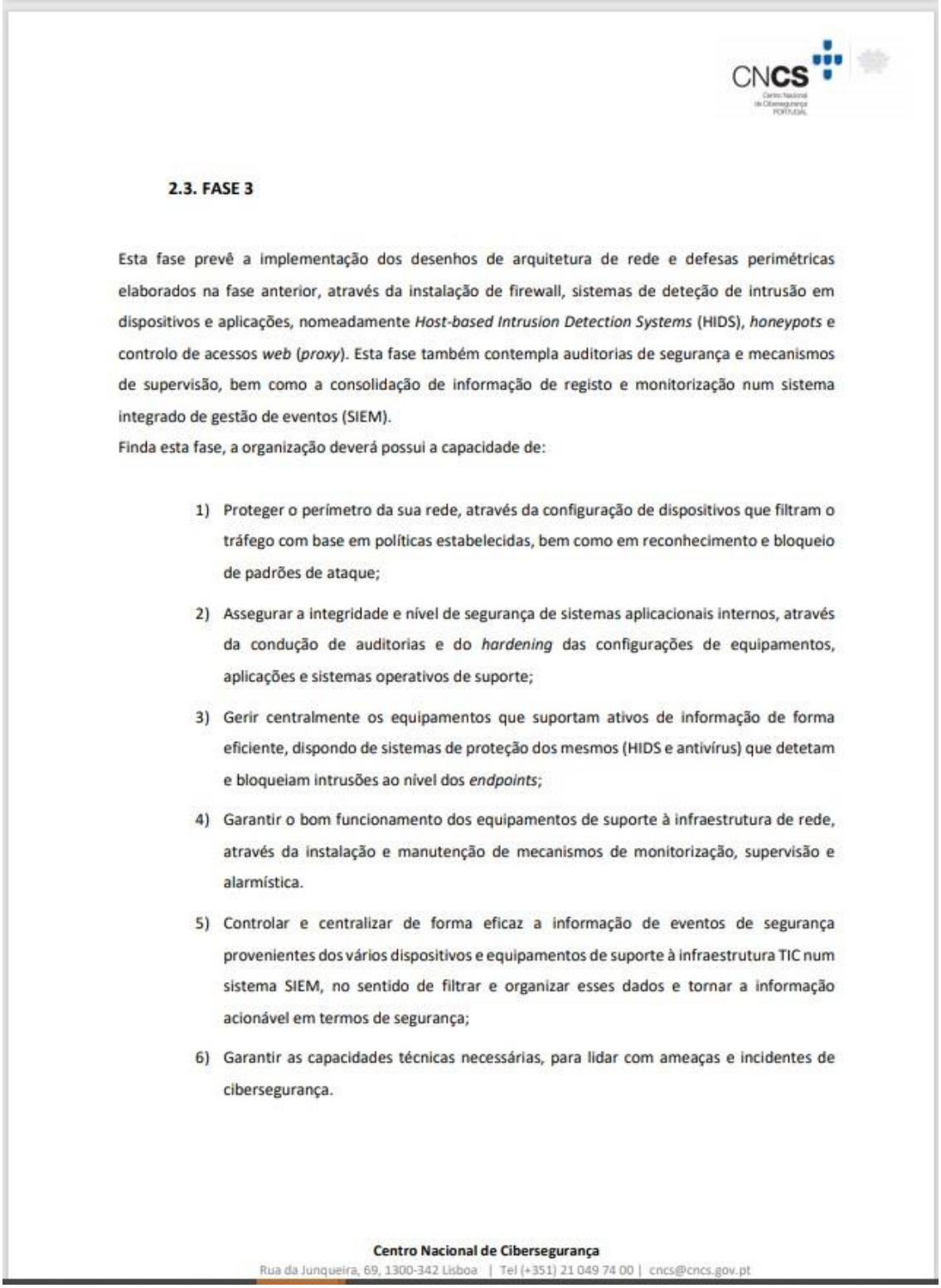
**Resposta:** "Não. A Ciberdiplomacia não é utilizado pelo GNS.
São utilizadas as ferramentas que anexei, os memoranduns com entidades publicas, a realização dos C-Days, etc.
O GNS/CNCS tem tido algumas interações como o Embaixador nomeado para esta função e alguma coordenação tem sido feita nesta área durante a PPUE21.
Tenho pouca visibilidade sobre este assunto e poderei estar a fornecer informação errada.

Envio link para este relatório muito importante*."

*Consultar anexos B.

# B - Quadros e figuras

## B.1 - Quadro de referencia de Cibersegurança do CNCS



### 2.3. FASE 3

Esta fase prevê a implementação dos desenhos de arquitetura de rede e defesas perimétricas elaborados na fase anterior, através da instalação de firewall, sistemas de deteção de intrusão em dispositivos e aplicações, nomeadamente *Host-based Intrusion Detection Systems* (HIDS), *honeypots* e controlo de acessos *web* (*proxy*). Esta fase também contempla auditorias de segurança e mecanismos de supervisão, bem como a consolidação de informação de registo e monitorização num sistema integrado de gestão de eventos (SIEM).

Finda esta fase, a organização deverá possui a capacidade de:

1) Proteger o perímetro da sua rede, através da configuração de dispositivos que filtram o tráfego com base em políticas estabelecidas, bem como em reconhecimento e bloqueio de padrões de ataque;
2) Assegurar a integridade e nível de segurança de sistemas aplicacionais internos, através da condução de auditorias e do *hardening* das configurações de equipamentos, aplicações e sistemas operativos de suporte;
3) Gerir centralmente os equipamentos que suportam ativos de informação de forma eficiente, dispondo de sistemas de proteção dos mesmos (HIDS e antivírus) que detetam e bloqueiam intrusões ao nível dos *endpoints*;
4) Garantir o bom funcionamento dos equipamentos de suporte à infraestrutura de rede, através da instalação e manutenção de mecanismos de monitorização, supervisão e alarmística.
5) Controlar e centralizar de forma eficaz a informação de eventos de segurança provenientes dos vários dispositivos e equipamentos de suporte à infraestrutura TIC num sistema SIEM, no sentido de filtrar e organizar esses dados e tornar a informação acionável em termos de segurança;
6) Garantir as capacidades técnicas necessárias, para lidar com ameaças e incidentes de cibersegurança.

**Centro Nacional de Cibersegurança**
Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | cncs@cncs.gov.pt