UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS V
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS
CURSO DE GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

MYREL RICHARD ALVES DOS SANTOS

CIBERSEGURANÇA E CIBERDEFESA NA ITÁLIA: O ATAQUE DE RANSOMWARE À REGIÃO DE LAZIO - ROMA EM 2021

JOÃO PESSOA
2024

MYREL RICHARD ALVES DOS SANTOS

CIBERSEGURANÇA E CIBERDEFESA NA ITÁLIA: O ATAQUE DE RANSOMWARE À REGIÃO DE LAZIO - ROMA EM 2021

Artigo acadêmico submetido ao Programa de Graduação em Relações Internacionais da Universidade Estadual da Paraíba, como parte dos requisitos para a obtenção do título de bacharel em Relações Internacionais.

Área de concentração: Defesa Cibernética, Segurança Cibernética, e Relações Internacionais.

Orientador: Prof. Dr. Filipe Reis Melo

Coorientadora: Profa. Dra. Thays Felipe David de Oliveira.

JOÃO PESSOA

2024

S237c Santos, Myrel Richard Alves dos.

Cibersegurança e ciberdefesa na Itália [manuscrito] : o ataque de Ransomware à região de Lazio - Roma em 2021 / Myrel Richard Alves dos Santos. - 2024.

35 p. : il. colorido.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) - Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, 2024.

"Orientação : Prof. Dr. Filipe Reis Melo, Coordenação do Curso de Relações Internacionais - CCBSA. "

"Coorientação: Prof. Dr. Thays Felipe David de Oliveira , UFPB - Universidade Federal da Paraíba "

1. Ciberespaço. 2. Ransomware. 3. Ciberdefesa. 4. Cibersegurança. I. Título

Elaborada por Livaneide da Silva - CRB - CRB15/638 BSC5/UEPB

MYREL RICHARD ALVES DOS SANTOS

CIBERSEGURANÇA E CIBERDEFESA NA ITÁLIA: O ATAQUE DE RANSOMWARE À REGIÃO DE LAZIO - ROMA EM 2021

Artigo acadêmico submetido ao Programa de Graduação em Relações Internacionais da Universidade Estadual da Paraíba, como parte dos requisitos para a obtenção do título de bacharel em Relações Internacionais.

Área de concentração: Defesa Cibernética, Segurança Cibernética, e Relações Internacionais.

Aprovado em: 27/06/2024.

BANCA EXAMINADORA

Filipe Reis Melo (Orientador)
Universidade Estadual da Paraíba (UEPB)

Lucila Gabriella Maciel Carneiro Vilhena
Universidade Estadual da Paraíba (UEPB)

Thays Felipe David de Oliveira
Universidade Federal da Paraíba (UFPB)

LISTA DE FIGURAS

SUMÁRIO

Cibersegurança e ciberdefesa na Itália: o ataque de ransomware à região de lazio - roma em 2021

Cybersecurity e cyberdefence in Italia: l'attacco ransomware alla Regione Lazio-Roma nel 2021

Myrel Richard Alves dos Santos[1]

RESUMO

O artigo visa analisar o ataque de *ransomware* contra os sistemas de informática da região de Lazio no ano de 2021. Sendo assim, é possível identificar o seguinte problema de pesquisa: qual a importância de investimento em ciberdefesa e cibersegurança para a Itália? Com a constante ameaça é necessário entender essa necessidade e identificar possíveis soluções utilizando tecnologias avançadas como *Blockchain* e Inteligência Artificial. A metodologia de estudo de caso presente, através da técnica de explanação, visa identificar como ocorreu o ataque, levantando dados sobre o acontecimento, analisando o caso e fornecendo conclusões sobre o problema, para que seja possível entender como foi solucionado e qual a velocidade de resposta. Entre as principais conclusões, destacamos que a Itália tem investido na proteção do ciberespaço, graças a isso os dados dos sistemas não foram totalmente perdidos devido aos *backups* realizados. Entretanto, novas formas de invasão serão sempre desenvolvidas, comprovando que, caso não haja uma frequência em investimento, os ataques cibernéticos continuarão evoluindo até suas consequências serem irreversíveis. As tecnologias apresentadas podem auxiliar na proteção e resposta impossibilitando o aumento dos danos causados.

Palavras Chave: Ciberespaço; *Ransomware*; Ciberdefesa; Cibersegurança.

[1] Formado em Técnico de Informática no Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN). Graduando em Relações Internacionais pela Universidade Estadual da Paraíba (UEPB). Atualmente trabalha na área de comércio exterior e tem a respectiva área de interesse: Estudo de segurança cibernética na Itália. Subárea de interesse: Segurança cibernética, defesa cibernética, Governança de TI e desenvolvimento de software. Endereço eletrônico: myrelrichard20@gmail.com

SOMMARIO

L'articolo si propone di analizzare l'attacco *ransomware* ai sistemi informatici della Regione Lazio nel 2021. Con questo è possibile il seguente problema di ricerca: quanto è importante l'investimento in *cyber-defence* e *cyber-security* per l'Italia? A fronte di una minaccia costante, è necessario comprendere questa esigenza e individuare possibili soluzioni utilizzando tecnologie avanzate come la *Blockchain* e l'Intelligenza Artificiale. La presente metodologia di studio di caso, utilizzando la tecnica della spiegazione, mira a identificare come si è verificato l'attacco, raccogliendo dati sull'evento, analizzando il caso e fornendo conclusioni sul problema, in modo che sia possibile capire come è stato risolto e quanto velocemente è stato risposto. Tra le principali conclusioni, si evidenzia che l'Italia ha investito nella protezione del cyberspazio, grazie alla quale i dati presenti sui sistemi non sono andati completamente persi grazie ai *backup* effettuati. Tuttavia, nuove forme di intrusione saranno sempre sviluppate, a dimostrazione del fatto che, in assenza di investimenti regolari, gli attacchi informatici continueranno a evolversi fino a quando le loro conseguenze saranno irreversibili. Le tecnologie qui presentate possono aiutare nella protezione e nella risposta, rendendo impossibile l'aumento dei danni causati.

Parole chiave: Cyberspazio; Ransomware; Cyberdefence; Cybersecurity.

1 CONSIDERAÇÕES INICIAIS

O ciberespaço é uma terminologia utilizada para descrever o ambiente virtual formado por uma interconexão de computadores, redes de comunicação e sistemas digitais. Com o passar do tempo o termo vem ganhando um protagonismo considerável nas relações internacionais, trazendo consigo benefícios substanciais e também desafios jamais conhecidos e estudados anteriormente. Com a evolução tecnológica e a globalização, novas quebras de barreiras ocorreram entre Estados. Esse contexto deveria proporcionar aos países uma maior cooperação, criando novas parcerias para desenvolvimento. Entretanto, após o fim da Guerra Fria, o ciberespaço se torna um proporcionador de guerras através do mesmo espaço, conhecidas como guerras cibernéticas, isso ocorre pois não existe uma legislação acordada internacionalmente, assim como não tem limitação para proliferação de sistemas

que possam ser utilizados, e a inerente natureza de dupla utilização de tais dispositivos (Marrone, 2021).

Dentro desse contexto, Villar-Lopes (2017) traz em sua obra "Relações Internacionais cibernéticas (CiberRI): o impacto dos Estudos Estratégicos sobre o ciberespaço nas Relações Internacionais". A partir dos estudos do ciberespaço, surge a nomenclatura conhecida como "*software power*", esse termo, para Villar-Lopes (2017), ressignifica uma nova área de estudos dentro das relações internacionais, pois se trata do poder e do investimento tecnológico que um Estado tem para conseguir obter reconhecimento no sistema internacional.

A partir dos estudos das relações internacionais cibernéticas, a cibersegurança tem seu lugar de destaque, seu foco é no setor privado e tem objetivo de proteger a integridade e a disponibilidade dos sistemas privados e é uma área de grande importância para receber foco de investimentos. Segundo Villar-Lopes (2016), a ciberdefesa também tem seu lugar de destaque, a área se refere às estratégias, políticas e operações conduzidas pelo Estado ou até mesmo entidades governamentais para proteger os interesses nacionais contra ameaças cibernéticas e a infraestrutura crítica, envolve a proteção de redes governamentais, sistemas militares e infraestruturas críticas (como energia e comunicação).

A Itália, como membro do sistema internacional, está ciente da necessidade de investimento nas áreas apresentadas e já se pronunciou diversas vezes. Em 31 de março de 2017, o Primeiro Ministro Paolo Gentiloni Silveri declarou a adoção do Plano Nacional de Proteção Cibernética e Segurança Informática, a exibição do decreto se encontra no ANEXO A e ANEXO B do presente relatório. O plano visa a resolução do Comitê Interministerial para a Segurança da República, um comitê que estabelece diretrizes para a proteção cibernética nacional (Silveri, 2017).

No entanto, ataques de *ransomware* ainda são muito frequentes, sua definição pode ser entendida a partir de Hassan (2019, p. 25), "Um malware de computador que se instala silenciosamente na máquina do usuário", um *malware* é um tipo de software malicioso ou mal-intencionado, criado para causar dano a um sistema de computador, rede, roubar dados ou realizar qualquer tipo de ação prejudicial sem o consentimento do usuário. O significado está alinhado diretamente com os conceitos de Baldoni (2021), a sua atividade introduz restrições no uso de um dispositivo, por exemplo, criptografando os dados ou impedindo o acesso ao próprio dispositivo afetado. Os ataques de *ransomware* são muito comuns na Itália. Funcionam através do desenvolvimento de tecnologias de ataque cibernético, consideradas

armas complexas que podem comprometer o governo, a sociedade e instituições, deixando sistemas que dependem do *core business* altamente fragilizados.

Com a inserção do sistema internacional no ciberespaço, o surgimento de novos tipos de tecnologias se desencadeiam pois o espaço proporciona novos perigos com impacto tecnológico gerando vulnerabilidade. Dentre as diversas tecnologias emergentes que existem no mundo, serão apresentadas tecnologias como blockchain e de inteligência artificial, pois são benéficas para utilização em *software*, área de maior destaque quando se comparada ao hardware (Villar, 2017).

Fontes de extrema importância para a pesquisa são o Instituto Affari Internazionali com sua obra intitulada "Italy and Cyber Defence" por Marrone (2021). O instituto destaca com detalhes quando ocorreu o ataque, além de tratar de questões de ciberdefesa na Itália. Ademais, dados são utilizados diretamente de outras fontes italianas como o Conselho Universitário Nacional (CUN), um órgão consultivo do Ministério Italiano de Universidades e Pesquisa para identificação das áreas de estudo dos professores envolvidos no Cybersecurity National Laboratory (CINI), localizado nas principais universidades, institutos de pesquisa e academias militares do país. Estes, compreendem um total de mais de 800 professores e pesquisadores e estão espalhados por todo o país. No decorrer do artigo é possível encontrar discursos de figuras importantes como Nicola Zingaretti, membro da câmara de deputados da Itália no ano de 2021 e ex-presidente da região de Lazio, assim como Alessio D'amato, conselheiro de saúde da região de Lazio no ano de 2021.

Outra fonte de informação utilizada no desenvolvimento do estudo de caso foi o site Ilsole (2021), essa referência auxiliou na identificação de período de tempo que o ataque permaneceu ativo, e o Ciso Advisor[2], um site dedicado à cibersegurança, segurança da informação e ciberdefesa para trazer informações críticas sobre a evolução de ameaças cibernéticas e como se defender de possíveis ataques. O site do governo italiano foi outra fonte de informação utilizada, referente às medidas de cibersegurança adotadas pelo governo. A medida foi divulgada pelo Primeiro Ministro Paolo Gentiloni Silveri (2021), que declarou a adoção do Plano Nacional de Proteção Cibernética e Segurança Informática.

O artigo tem como objetivo principal analisar a necessidade de investimento em cibersegurança e ciberdefesa para a Itália e entender dois tipos de tecnologias e suas utilizações na detecção e reposta contra ataques de *ransomware*. Esses objetivos serão

[2] Seus fundadores são Erivelto Tadeu – Cofundador do Ciso Advisor, jornalista e é especializado em setores como internet, TI, telecomunicações, mercado de capitais e financeiro, tendo Alexandre Gerdelmann como Gerente Comercial, um especialista em mídias digitais e imprensa, com foco nos setores de Tecnologia da Informação e de Telecomunicações (Ciso Advisor, 2018)

inseridos dentro do contexto do estudo de caso de ataque de *ransomware* na região de Lazio. Ao final do artigo, serão apresentados possíveis utilizações das tecnologias emergentes conhecidas como Inteligência Artificial e Tecnologia Blockchain para análise de viabilidade dos seus papéis como identificadores e solucionadores de possíveis problemas que possam surgir. Essas duas tecnologias serão apresentadas a partir dos estudos de autores como Bovério e Silva (2018), Romar (2022) e Abbass (2021).

A metodologia deste artigo tem como foco o estudo de caso único. Robert K.yin (2001) informa que o escritor pode se apoiar em quatro técnicas principais, sendo elas: (1) adequação ao padrão, (2) construção da explanação, (3) análise de séries temporais e (4) modelos lógicos de programa. Na adequação padrão, existe uma comparação do padrão empírico baseado na experiência versus a base prognóstico, em resultado, se esses padrões coincidirem, temos uma pesquisa efetiva; na construção da explanação, o objetivo não é construir um estudo e sim desenvolver ideias para um novo estudo; análise de séries temporais é uma série baseada em experimentos e pesquisas experimentais; modelos lógicos de programa é uma combinação de técnicas da adequação ao padrão e análise de séries temporais.

É destacado por Robert K.yin a necessidade de se iniciar um estudo de caso a partir de seu referencial teórico. Villar-Lopes (2016-2017), Alison (2015) e Baldoni (2018) foram autores utilizados para conceituar o ciberespaço, as Relações Internacionais Cibernéticas e a importância de investimento em tecnologia na área de cyber para um país. Baldoni (2018), Diretor da Agência Nacional de cibersegurança até março de 2023, e Villar-Lopes (2016-2017) serão responsáveis pela definição dos conceitos de ciberdefesa e de cibersegurança. Os dois autores têm conceitos similares de cibersegurança e de defesa cibernética - vale ressaltar que esses dois termos possuem definições diferentes pois a cibersegurança tem seu foco no setor privado, protegendo a integridade e disponibilidade dos sistemas privados, ja a defesa cibernética ou ciberdefesa são estratégias, políticas e operações conduzidas pelo Estado - podendo proporcionar a utilização do seu significado puro, no entanto, sem aprofundamento nos conceitos de Villar-Lopes (2016-2017), pois o estudo de caso será feito através de uma perspectiva italiana.

O método se baseia na técnica de construção da explanação com o objetivo de analisar os dados do estudo de caso construindo uma explanação sobre o caso segundo Robert K.yin (1982b apud Robert K.yin, 2001). No capítulo de coleta de evidência, existem princípios para se fazer uma coleta. O autor mostra a importância da coleta de evidências e ratifica que é necessário entender que, um estudo de caso pode surgir de 6 fontes distintas: documentos,

registro em artigos, entrevista, observação direta, observação participante e artefatos físicos. O uso dessas 6 fontes requer procedimentos diferentes importantes para o trabalho de coleta de dados. São necessárias duas ou mais fontes que convirjam em relação aos mesmos conjuntos de fatos ou descobertas. As ligações entre as fontes ao decorrer do artigo a partir desta metodologia estão alinhadas e se complementam para chegar a uma só conclusão referente ao estudo de caso.

A análise será realizada a partir da utilização dos materiais apresentados, tais como a revisão de reportagens gravadas, artigos e relatos de entrevistas, para desenvolver um método de explanação em 4 etapas, sendo elas: (1) identificação de um problema de pesquisa, (2) levantamento de dados, (3) análise de contexto e (4) conclusões sobre o problema. Com o método de análise foi possível identificar que a Itália tem tomado medidas de investimento em tecnologias de resposta contra ataques cibernéticos. Desde a criação de uma medida oficial de segurança adotada pelo governo, inúmeras mudanças surgiram.

O estudo de caso terá como foco o ataque de *ransomware* ocorrido na região de Lazio em 2021. A coleta de dados presente no artigo é referente a documentos e registros em artigos. O HSS Cybersecurity Program (2021) foi utilizado como comprovante de informações da ocorrência do ataque como a data do incidente e a data da solução, assim como o que foi feito para solucionar o problema de forma superficial, segundo a fonte o ataque ocorreu durante o período de 31 (trinta e um) de julho e 1 (primeiro) de agosto de 2021. O artigo relatado pela HHS Cybersecurity Program (O programa de cibersegurança do HHS) (2021) identifica que o ataque realizado por um RansomEXX, o *ransomware* desativou os sistemas de TI da região, relata também o possível envolvimento do *ransomware* LockBit 2.0.

O artigo está dividido em capítulos, cada um deles irá aprofundar de forma gradativa na temática principal da pesquisa que é a segurança e defesa cibernética italiana. O capítulo “Surgimento do ciberespaço nas relações internacionais” tem o intuito de destrinchar os conceitos que serão aqui utilizados dentro das Relações Internacionais cibernéticas e alinhar as fontes brasileiras como Gills Vilar Lopes com autores italianos principalmente Roberto Baldoni. “Segurança Cibernética na Itália” ou “Cibersegurança na Itália” trata sobre o quão relevante a Itália considera o investimento em método de segurança e defesa cibernética para o país, além disso, ressalta a veracidade e quantidade de ataques cibernéticos que ocorrem para proporcionar ênfase ao quanto deve ser introduzido nas metas de um Estado o investimento no ciberespaço, o capítulo tem objetivo de também de analisar o ocorrido na

região de Lazio e verificar a viabilidade do uso de tecnologias para melhorar o trabalho de detecção e resposta contra o *ransomware*.

2 O SURGIMENTO DO CIBERESPAÇO NAS RELAÇÕES INTERNACIONAIS

2.1 O Ciberespaço

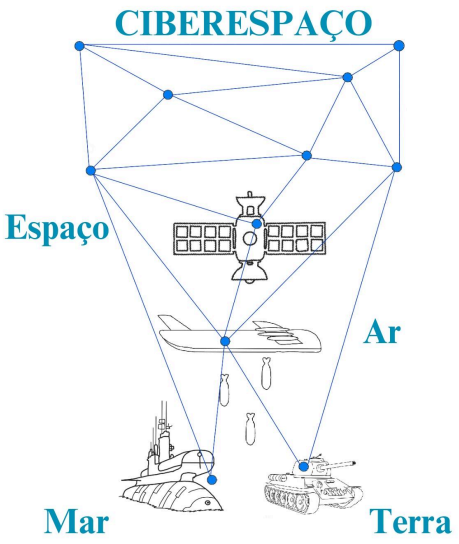
Segundo Alison (2015), quando nos referimos ao ciberespaço, não se trata apenas de um espaço artificial, o real significado tem um processo de domínio contingente, real. O espaço virtual não são apenas manifestações fictícias, é um espaço concreto de grande informação operando por meio de conexões computacionais, entretanto, de acordo com o objetivo de utilização desse espaço, sua concepção se altera. Desde a designação mais básica, o ciberespaço se revela como uma realidade artificial e virtual, multidimensional, acessível através de computadores interligados por uma rede global. A engenharia do espaço cibernético não se limita a uma única perspectiva subjetiva, mas é expressa por meio de uma troca coletiva de ideias e conceitos.

A utilização gratuita de um espaço virtual facilita o compartilhamento instantâneo. Nesse contexto, a virtualidade não simplifica o real ao abstrato ou o abstrato ao concreto, mas identifica a emergência de um novo domínio. A tecnologia cibernética, encontra-se imersa em uma rede em constante evolução, permeada por complexas relações e interações. A experiência é situada através do computador, inserindo-se em uma noosfera participativa. Os sistemas do ciberespaço operam de maneira independente do ambiente de origem, e a geometria que os delineia pertence a estruturas autônomas que moldam a totalidade da estrutura (Alison, 2015).

Com a descoberta do ciberespaço e as área das Relações Internacionais Cibernéticas, um novo contexto surge com novas nomenclaturas e estudos na área, vindo principalmente de países reconhecidos como verdadeiras potências cibernéticas, sendo exemplos deles: Estados Unidos da América (EUA), China e Rússia (Villar-Lopes, 2016). Isso ocorre pois o ciberespaço é um local de interação direta e indireta, que pode atingir desde pessoas até países. Muitos governos têm adotado a cibersegurança em suas agendas, pois o ciberespaço se transforma no quinto domínio estratégico para ações militares, sendo os cinco identificados como: terrestre, marítimo, aéreo, espacial e cibernético. O desenho abaixo demonstra as dimensões dos domínios e a influência do espaço cibernético onde o submarino

representa o domínio marítimo, o tanque representa o terrestre, avião - aéreo, satélite - espaço e por último o espaço cibernético.

Figura 1 - Domínios estratégicos para ações militares.



Fonte: Elaboração própria.

O grande impacto causado pelo quinto domínio é perceptível em muitos casos como por exemplo a primeira arma cibernética conhecida como *stuxnet*. Segundo Zetter (2014), worm foi capaz de infectar o sistema operacional de centrífugas de enriquecimento de urânio em Natanz no Irã, o ataque causou efeitos cinéticos pois atrasaram o processo de atividade das centrífugas deixando mil, dentre as 5 mil existentes, inativas. É possível também entender as razões desse ataque tendo objetivos políticos, pois um worm tão bem estruturado como este só poderia ser desenvolvido com o investimento de algum país ou até mesmo mais de um, esse apoio de um Estado é fato comprovador do termo que será apresentado neste artigo, o *software power*.

É ressaltado por Zetter (2014) e Lindsay (2013), evidências de possíveis motivações para comprovar a atividade de investimento dos Estados Unidos e de Israel no ocorrido. Além de Israel e Estados Unidos possuírem o desenvolvimento tecnológico, também possuem motivos, pois os 3 países relacionados no caso possuem um grande histórico de desavenças.

> Pouco tempo depois da descoberta pública do Stuxnet, as especulações começaram a recair sobre os Estados Unidos e/ou Israel. Assim que o nível de sofisticação técnica foi apreciado e divulgado pela comunidade de segurança informática, as preocupações com hackers solitários e bandos terroristas puderam ser excluídas por falta de meios. Os Estados com capacidade de guerra cibernética, como a Rússia ou a China, não tinham motivos convincentes, embora alguns tenham tentado invocar um caso de conspiração. Israel e os Estados Unidos, pelo contrário, estavam bem dotados tanto de meios como de motivos (Lindsay, 2013, p. 400).

Outro caso que pode ser utilizado é o ataque da Coreia do Norte no ano de 2014 contra a Sony Corporation. Foram invadidos diversos *e-mails* e dados pessoais de clientes foram expostos. O ataque foi realizado no mundo cibernético, entretanto teve consequências no mundo real, nos setores econômico-financeiros, pois a multinacional japonesa na National Association of Securities Dealers Automated Quotations (NASDAQ) perdeu sua valorização, afetando também os Estados Unidos que possuíam ações na empresa, assim como muito outros países (Villar-Lopes, 2017)

O ciberespaço é para Baldoni (2018) a coisa mais complexa que o ser humano já construiu até o ano de 2018. Essa complexidade está submetida a inúmeros fatores negativos que podem ocorrer devido a toda a disponibilidade de acesso, tais como erros de software, configurações de máquinas incorretas e pontos fracos em protocolos de defesa. Essa vulnerabilidade é explorada a todo momento por criminosos cibernéticos, principalmente na tentativa de roubar dados confidenciais ou até mesmo para simplesmente causar danos a um inimigo comum.

2.2 As Relações Internacionais Cibernéticas

A partir dos estudos de Villar-Lopes (2021) e com a entrada do sistema internacional no ciberespaço, surge o campo de estudo das relações internacionais cibernéticas (CiberRI). Essa área destaca que com o processo de disputas hegemônicas constantes entre os Estados, é necessário a existência de pesquisadores, analistas e a formação de uma nova área nas Relações Internacionais, haja vista, o ciberespaço tem se tornado cada vez mais uma pauta entre os países por se tratar de um local ainda sem uma constituição exata de regras.

A importância dos estudos relacionados ao ciberespaço se torna um debate a partir do momento em que é necessário a criação de uma área para traçar um sistema de desenvolvimento de estudos que podem influenciar diretamente nas relações entre países. Todo o estudo desenvolvido por um ciber internacionalista pode ser capaz de observar, analisar e sintetizar fatos e acontecimentos cibernéticos que impactam as RI e/ou às relações internacionais e vice-versa (Villar-Lopes, 2016)

Assim como o campo pode afetar a relação entre países de forma positiva, consequências negativas também podem surgir, pois o ciberespaço é um lugar ainda com uma abertura considerável para crimes com um baixo retorno de consequências para os desenvolvedores de ataques cibernéticos. A seguir serão apresentados exemplos destacados por Villar-Lopes (2016) em sua tese de doutorado intitulada “Relações Internacionais Cibernéticas (Ciberri): Uma Defesa Acadêmica A Partir Dos Estudos De Segurança Internacional”, que mostra como o ciberespaço pode influenciar diretamente nas Relações Internacionais a partir de diferentes campos da área com consequências consideráveis.

(1) No comércio e na cooperação internacional, na venda de produtos e serviços ilícitos, esse problema não se resume apenas a questões tecnológicas, mas também se referem a problemas relacionados à dificuldade de cooperação entre agentes governamentais como ministérios públicos, polícias e agências de inteligência, além de organizações como a Interpol (organização internacional que facilita a cooperação policial mundial e o controle do crime).

(2) Relacionadas à diplomacia, as atividades de espionagem cibernética são muito comuns atualmente, o que afeta diretamente relações entre grandes potências mundiais. As consequências da espionagem repercutem no país durante muito tempo, principalmente quando documentos sigilosos são encontrados e até mesmo revelados em sites na internet. Isso se reflete em diversos aspectos negativos como a desconfiança e a tensão diplomática, danos à segurança nacional, prejuízos econômicos, impactos nas relações bilaterais e até

mesmo comprometimento na legitimidade e credibilidade internacional em relação aos países envolvidos na atividade de espionagem.

(3) Também é mencionado na obra relações no âmbito econômico com o uso das moedas virtuais, mais conhecidas como criptomoedas, que têm suas premissas questionadas devido a sua fonte monetária vinda de *bytes*.

> Se permite questionar premissas do sistema financeiro internacional e da própria Economia Política Internacional, com uma fórmula monetária lastreada não no ouro nem em outra moeda – ou conjunto delas –, mas, sim, em bytes, por meio de sua mineração. (Villar-Lopes, 2016, p. 21).

Saindo da instrução sobre cibersegurança e ciberdefesa de Villar-Lopes (2019) e (2016), Baldoni (2018) considera que a cibersegurança deve abarcar diferentes áreas, impactando múltiplos aspectos da sociedade. Apesar disso, os termos anteriormente utilizados, ainda podem ser considerados no seu significado principal. Baldoni (2018) utiliza também utiliza os mesmos termos com seus respectivos significados, sendo a cibersegurança atuante na prevenção e na proteção contra ameaças digitais, e a defesa cibernética responsável pela detecção, resposta e recuperação de ataques cibernéticos. A obra "Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici" de Baldoni (2021) considera vários aspectos da cibersegurança, desde a definição das infraestruturas e centros necessários para estruturação de uma cibersegurança até ações de investimento em tecnologias a serem desenvolvidas para uma melhor defesa.

2.3 Software Power

O mundo está cada vez mais inserido dentro do ciberespaço, com o acesso à novas tecnologias, novas estratégias de ataque são aplicadas por outros Estados para coleta de informações e também métodos de ataque para impedir o desenvolvimento de outros países. Dentro da área de segurança, o país precisa desenvolver melhor suas tecnologias de resposta contra ataques dessa magnitude, o conceito de Vilar (2016) , "*Software power*", destaca a necessidade de um investir em defesa cibernética para situações de tentativa de um Estado impor sua soberania através do campo cibernético.

Software power se trata de um conceito que destaca a capacidade de um Estado na obtenção de poder de *software* para obter influência e controle do ciberespaço. Villar-Lopes (2016) disserta sobre a extrema competitividade e disputa na área de segurança internacional, tornando necessário que os países comecem a investir em defesa cibernética. Assim como ocorre a melhora de tecnologias para ataque cibernético, também é necessário investimentos para garantir a defesa de um país contra os possíveis malwares que possam surgir (Villar-Lopes , 2021).

Software power trata de uma intenção, sendo esta política, que surge a partir do ciberespaço, para entendermos o conceito é necessário entender também as capacidades que a tecnologia tem de dar suporte à força bélica de um Estado. Villar-Lopes (2017) utiliza o conceito de software power por duas razões, a primeira é por uma aceitação universal do termo, o segundo motivo é devido ao seu significado em português não ter uma exatidão ao ser utilizado, "Poder de computação" não é o real significado do termo, haja vista, se trata de um atributo e não um adjetivo ou substantivo do poder como Nye Jr Nye Jr (2004; 2011b) faz ao utilizar os termos *Soft Power* e *Cyber Power* pois o termo Software Power remete mais ao poder e não diretamente ao *software*.

Na tentativa de alcançar poder os países geram constantes ataques cibernéticos para diferentes objetivos, motivados por questões políticas ou geopolíticas, interesses econômicos, ciberespionagem ou atividades de grupo cibernéticos. Nessa tentativa de impor a soberania no sistema internacional dentro do mundo cibernético se enquadra a área de CiberRI, trazida na obra "Relações Internacionais cibernéticas (CiberRI): o impacto dos Estudos Estratégicos sobre o ciberespaço nas Relações Internacionais. Segundo Villar-Lopes (2021), às Relações Internacionais Cibernéticas identificam a existência da necessidade de uma área de estudo nas Relações Internacionais onde se destacam as análises existentes no contexto do quinto domínio.

3 SEGURANÇA CIBERNÉTICA NA ITÁLIA

3.1 Segurança Cibernética na Itália

Com a latente tentativa de ataque cibernético presente nas Relações Internacionais, o Estado precisa prover segurança e estudos na área para sua nação. A Itália não fica de fora dessa análise. Segundo Matassa (2022), a União Europeia (UE) não foi uma das primeiras instituições a adquirir plena consciência da necessidade de se preparar num contexto de

segurança cibernética. Vale ressaltar que, segundo CINI (2023), a Itália teve uma consciência tardia sobre a importância do tema, mas não anula o fato do país possuir ótimos mecanismos de defesa originais. Nesse sentido, segundo o site Best.it (2015) o Consórcio Nacional Interuniversitário de Informática (CINI) foi estabelecido em 6 de dezembro de 1989, e é formado por 51 universidades públicas italianas com mais de 1.300 professores universitários envolvidos nos setores de informática e sistemas de processamento de informações.

Segundo CINI (2023), o laboratório CINI tem como objetivo principal a colaboração para concretização de um ecossistema nacional italiano de cibersegurança. Essa meta visa ser alcançada através de uma maior promoção de investigação e formação, através de uma perspectiva interdisciplinar e multidisciplinar que favorece a realização de atividades conjuntas entre pesquisas públicas e privadas. Objetivos como esses precisam ser traçados, pois um país que não possui a cibersegurança no centro de suas estratégias é um país que deixa um espaço vulnerável para a própria prosperidade e independência.

Baldoni (2018) traz a obra introduzida, no fim do ano de 2015, pelo Laboratório Nacional de Cibersegurança do CINI. Foi criado um livro branco como iniciativa para explicar e descrever os principais desafios de segurança cibernética que a Itália enfrentará nos próximos 5 anos. O principal foco do livro são os riscos decorrentes de um ataque cibernético. No livro, diversos aspectos da cibersegurança são destacados, desde a definição e infraestrutura de centros necessários para organizar as ações e as tecnologias a serem desenvolvidas para serem protegidas da melhor forma possível, até a proposta de um conjunto de ações horizontais para treinamento, conscientização e gerenciamento de riscos. A pesquisa apresentada pelo CINI em seu livro branco está diretamente ligada à procura e ao estudo de soluções para desafios da área de segurança cibernética (Baldoni, 2018).

Os âmbitos de atuação destacadas no livro branco são agrupados em cinco áreas operacionais: (1) Infrastrutture e Centri, essa área visa estudar ferramentas e ações de proteção da rede nacional da internet e *data centers*; (2) Azioni Abilitanti, que está voltada para o ciclo de gerenciamento de ameaças desde a proteção de aplicativos nacionais críticos até a criação de um banco nacional de ameaças para defesa contra ataques cibernéticos e gestão de risco; (3) Tecnologie Abilitanti, focado em projetos que visam fortalecer algumas das tecnologias básicas a serem utilizadas para proteger dados, limitar ataques e seus efeitos, aumentando a capacidade dos sistemas através de soluções voltadas para a segurança, tecnologias como a *blockchain* por exemplo; (4) Tecnologie da proteggere, área que apresenta ferramentas usadas na proteção de tecnologias de comunicação sem fio, serviço de nuvem, lógicas de sistemas funcionais, sistemas de controle industrial, robôs e muitos outros;

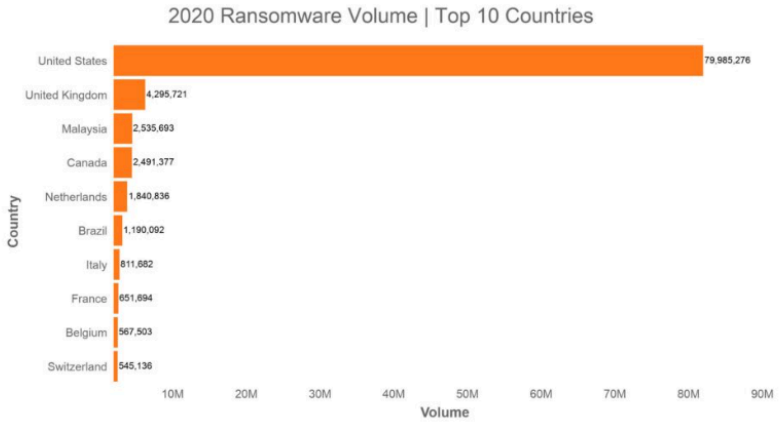
e por último (5) Azioni Orizzontali, cujo objetivo é garantir proteção de dados pessoais, aumentar o nível de conhecimento e de competência através de projetos que melhoram o gerenciamento de riscos em nível empresarial.

Um documento estruturado é extremamente necessário, pois ataques cibernéticos têm impactos que deixam marcas. Foi relatado em maio de 2017 por ministros das finanças e governadores dos bancos centrais dos países do G7, em uma reunião em Bari, que se faz necessário uma base de informações pública sobre ataques cibernéticos. “Reconhecemos que os incidentes cibernéticos representam uma ameaça crescente às nossas economias, e são necessárias respostas políticas que envolvam todo o sistema de produção. Com base em dados confiáveis, imparciais, abrangentes e amplamente acessíveis. As definições, as metodologias de coleta e o compartilhamento de dados, quando apropriado, devem ser coordenados e consistentes entre países e setores, para que os resultados sejam comparáveis” (Apud, Baldoni, 2018).

Segundo o presidente da Comissão Europeia, Jean-Claude Junker, no seu discurso sobre o Estado da União, em 13 de setembro de 2017, a cibersegurança se enquadra em segundo no ranking de preocupações da Europa, vindo logo depois das mudanças climáticas e antes da imigração. Isso ocorre pois existem diversas ameaças que um estado está suscetível como por exemplo o controle sub-reptício de serviços de infra-estruturas críticas e o roubo de propriedade intelectual ou de informações cruciais para a sobrevivência de uma empresa (Baldoni, 2018).

A Itália ainda em 2020 se encontrava no ranking entre os 10 países que mais sofrem ataque de *ransomware*, isso deixa claro a necessidade de investimento do país em ciber defesa, haja visto que tecnologias precisam ser instauradas e atualizadas sempre que possível para defesa contra ataques cibernéticos deste nível. De acordo com o Ciso Advisor (2020), segundo a figura 3 o país foi alvo de em média 811,682 (oitocentos e onze mil seiscentos e oitenta e dois) ataques de *ransomware*.

Figura 2: Volume de *Ransomware* | Top 10 países (ano 2020)



Fonte: Ciso Advisor, 2020.

Os dados apresentados auxiliam na comprovação da necessidade de investimento que a Itália precisa ter em sua ciberdefesa, haja vista, uma quantidade considerável de malwares são redirecionados para o país anualmente. A necessidade de investimento em defesa cibernética se torna ainda mais necessária na região de Lazio pois foi um ataque envolvendo diretamente a população, haja vista, afetou o sistema de vacinação contra o COVID no ano de 2021.

O *ransomware* é considerado uma das armas mais perigosas do mundo cibernético por ser altamente avançado em tecnologia, podendo desencadear um reflexo de alerta não só em pessoas como também em governos e instituições. Esse tipo de malware tem sido desenvolvido há muito tempo, e tem a finalidade principalmente de obter lucro, entretanto, para autores como (Pimentel, 2021) pode também ser criado a partir de causas sociais ou ideológicas.

Na maioria das vezes o ataque envolve o bloqueio de acesso a arquivos, sejam eles confidenciais ou não, desencadeando um ataque às contas de armazenamento em nuvem. Essas ações têm o objetivo de exigir um pagamento de resgate do sistema para que o criador remova o vírus do computador, para assim tornar possível o acesso aos dados novamente (Pimentel, 2021).

3.2 Análise do acontecimento

Para comprovação e detalhamento de que ataques cibernéticos causam danos extremamente perigosos, em 2021, os sistemas de TI da região de Lazio sofreram um ataque cibernético de *ransomware* impactando a segurança cibernética na região. O ataque na região

representou um grande alerta para a Itália, isso ocorre pois a região de Lazio é a segunda região mais populosa de toda a Itália e também é onde está a capital do país, Roma. O ataque buscou atingir os dados da campanha de vacinação contra o COVID-19 (Marrone, 2021).

O presidente da região, Nicola Zingaretti, pronunciou-se em seu facebook confirmando a data do ocorrido. Segundo ele, não foram encontrados os responsáveis pelo ataque até a primeira semana do evento Os arquivos do *data center* foram bloqueados, no entanto, as vacinações continuaram normalmente para quem já tivesse marcado uma consulta anterior ao ataque de *ransomware*.

O país tem se desenvolvido em tecnologia e infraestruturas críticas, mas a dependência de importação de tecnologia e equipamentos é uma variável que não se pode menosprezar, haja vista que a dependência digital expõe o país a uma gama de ameaças cibernéticas. A adoção de tecnologias como a Internet das Coisas (IoT), a inteligência artificial e a computação em nuvem tem proporcionado avanços dentro do mundo cibernético, gerando uma maior segurança, entretanto, também pode gerar armas como o *ransomware*.

Essa arma pode ser caracterizada em duas classes principais, "*Locker-ransomware*" e "*Crypto-ransomware*". O "*Locker-ransomware*" na maioria dos casos bloqueia o acesso à interface do usuário impedindo o acesso à qualquer recurso do computador, para resgatar o computador nesses casos é necessário restauração, o Locker se torna muito eficaz em dispositivos de interação limitada entre os usuários. O "*Crypto-ransomware*" é aplicado em situações onde dados de computador podem ser criptografados removendo o acesso do usuário, sendo permitido apenas com a utilização de uma chave desconhecida, este malware causa mais danos que o Locker haja vista os dados não são restaurados após a retirada. Com isso, por ser caracterizado como perigoso e ter uma entrada na máquina de destino através de uma forma totalmente silenciosa, fica claro a necessidade de desenvolvimento de métodos para identificação da instalação do malware (Pimentel, 2021).

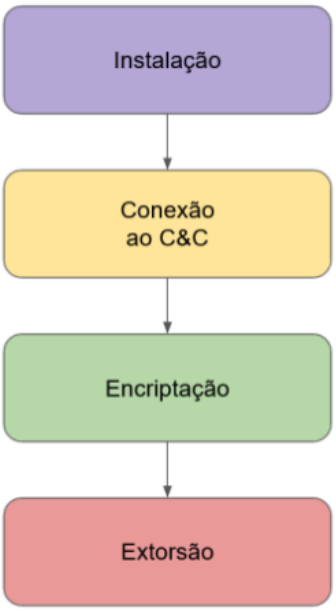
Para que um ataque de *ransomware* ocorra, é necessário seguir uma certa quantidade de etapas de realização. Existem diversos meios onde o malware pode se instalar, através de emails maliciosos atualmente conhecidos como Phishing[3], e os *exploit kits* que são sistemas de software instaladores para procura de vulnerabilidades no sistema, entretanto, sua real finalidade é instalar um arquivo malicioso e os downloads drive-by sites mal intencionados que executam códigos maliciosos, na imagem abaixo coletada do artigo "Estudo de Métodos

[3] O phishing é um tipo de ciberataque que utiliza ferramentas e passos especiais para obter informações sensíveis dos utilizadores (Sharma, 2007).

de Detecção¸ ao de *Ransomware* Utilizando Inteligência Artificial" é possível analisar de uma forma mais visível como funciona um ataque de *ransomware* (Romar, 2022).

Na figura a seguir, confira através de tópicos, os principais estágios que um *ransomware* passa até a sua instalação total em uma máquina:

Figura 3: Metodologia do ataque *ransomware*



Fonte: Romar (2022, p.3).

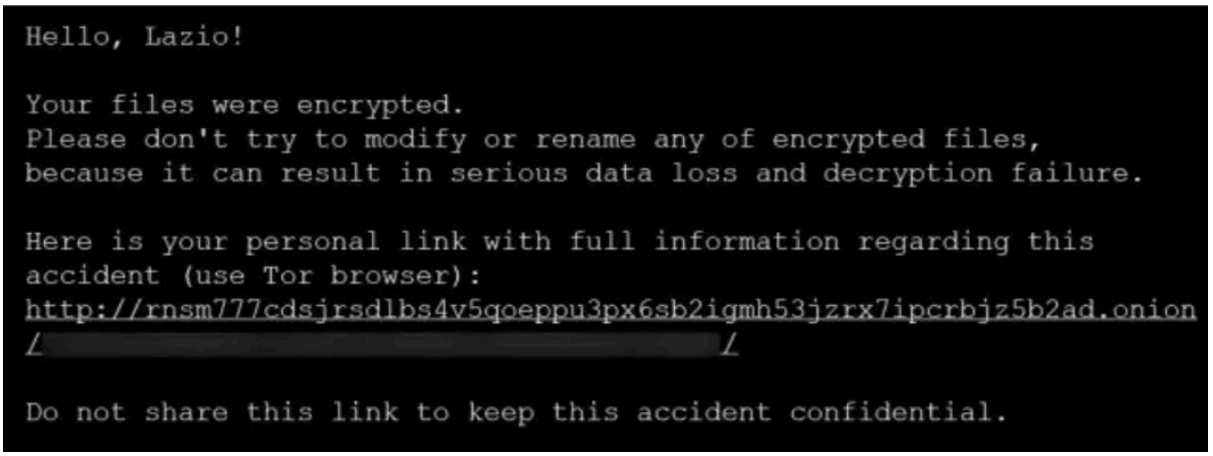
A execução do *malware* só irá ocorrer após o momento em que o arquivo estará na máquina. A área de conexão com o servidor de comando e controle (C&C) acontece quando é instalado no sistema, após esta etapa, é possível proceder a execução completa do *ransomware*. No estágio de encriptação, utiliza-se de criptografia de ponta para estabelecer uma ponte segura para o servidor de comando e controle, alguns utilizam métodos de criptografia simétrica enquanto outros preferem pela utilização de métodos de criptografia assimétrica (Romar, 2022).

O último estágio identificado como extorsão é a etapa onde o *ransomware* conseguiu criptografar os arquivos com a utilização de uma chave, Segundo Romar, 2022, pág. 4 " As chaves assimétricas usaram uma chave pública que pode criptografar, mas o processo de descriptografia requer a chave privada correspondente, que é armazenada apenas no servidor

de comando e controle" é a partir desse momento que a etapa de extorsão começam, pois para recuperar os arquivos através dessa chave é cobrado um valor para o dono do servidor.

Inicialmente o sistema da Lazio Crea foi totalmente desligado e a empresa informou que os dados de saúde, assim como dados financeiros e orçamentários estavam totalmente seguros. Os serviços gerais foram transferidos para nuvens externas para que pudessem ser utilizados o mais rápido possível (Ciso Advisor, 2021).O ataque ocorreu entre a noite de 31 de julho de 2021 e a manhã de 1° de agosto do mesmo ano. O conselheiro da saúde de Lazio no ano de 2021, Alessio D'Amato, afirma que o ataque começou logo após o vazamento das credenciais de um funcionário da empresa Lazio Crea, empresa responsável pelo gerenciamento de rede de computadores da região de Lazio, possibilitando que os criadores e organizadores do ataque cibernético fizessem login na VPN Lazio Crea, acessassem o site principal da empresa e implantassem o *ransomware* no Centro di Elaborazione Dati (CED). A mensagem implantada pelos criminosos que confirmam a instalação do *ransomwareEXX* se encontra na figura abaixo (HSS, 2021).

Figura 4: Nota de resgate de ataque de *ransomware* em Lazio



Fonte: HSS, 2021.

O link disponibilizado na mensagem após o ataque redireciona o usuário para um site na *dark web*, após clicar no link é possível entrar em contato com os criminosos. O *ransomware* que desativou os sistemas de TI da região é atualmente conhecido como RansomEXX, esse tipo de malware começou como uma variante que afetava apenas o sistema windows, responsável por sequestrar os dados da vítima, criptografar e exigir um resgate para que a chave de recuperação fosse enviada, mas posteriormente, foi possível

também afetar sistemas Linux a partir de uma modificação de códigos para explorar vulnerabilidades e funcionar de forma efetiva em diferentes ambientes e sistemas operacionais (FRANK, 2021).

Para entender mais sobre o ataque, é necessário analisar como funciona a partir de exemplos. As informações a seguir serão relatadas a partir de uma simulação de ataque em um sistema windows. Inicialmente, o *ransomware* é carregado de forma reflexiva, ou seja, é um malware sem arquivos, a invasão não ocorre através de instalação tradicional nos sistemas do computador, mas sim na memória RAM da máquina o que torna o malware ainda mais difícil de ser identificado, mesmo com sua dificuldade de detecção, a remoção pode ser fácil necessitando apenas de uma reinicialização, no entanto, dependendo do caso o *ransomware* pode criar tarefas agendadas para injetar o código na memória novamente, o que pode dificultar o processo de resgate. Isso ocorreu na região de Lazio, pois segundo a CNN (2021), os arquivos criptografados ainda podiam ser corrompidos pois as áreas afetadas foram isoladas. Entretanto, até as primeiras etapas de identificação do ataque, a porta de entrada do malware não foi identificada. Após a execução do arquivo, é possível descriptografar *strings* (dados utilizados para manipular e armazenar textos representados por uma sequência de caracteres, números, letras, espaços ou símbolos) para que seja possível o seu funcionamento (FRANK, 2021).

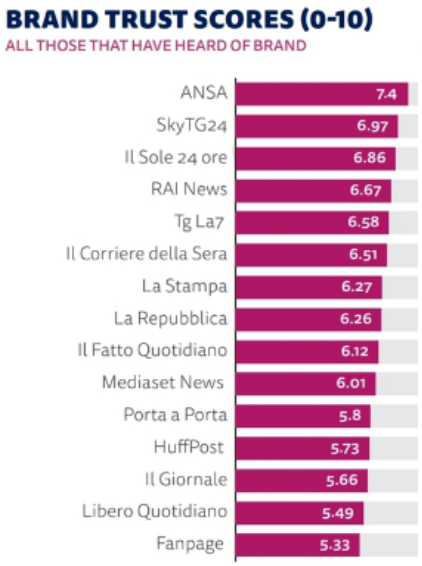
Além disso, segundo HSS Cybersecurity Program (2021), um investigador de segurança italiano desconhecido, informou ter provas sobre o envolvimento de outro tipo de *ransomware*, o LockBit 2.0. Ataques como esse têm se tornado muito comuns na Itália, pois ainda existem sistemas muito fragilizados que estão suscetíveis a ataques cibernéticos, segundo Chuck Everette (2021), diretor de defesa da segurança cibernética da empresa de segurança cibernética Deep Instinct Ltd., o ataque ao portal de vacinas da Lazio não é um incidente isolado. Como esse ataque faz parte de uma campanha mais ampla, ele deve ser motivo de mais preocupação para outras agências governamentais e organizações de saúde em todo o mundo. O foco da análise são os possíveis riscos ocorridos durante o ataque.

O *Health Sector Cybersecurity Coordination Center* (HC3 CTI) observou ataques cibernéticos recentes e semelhantes que afetaram a região de Lazio, na Itália, desde junho de 2021. Segundo o HSS (2021), o autor de língua inglesa 'Mastiff' anunciou dados de vacinação contra a COVID-19 de 7,4 milhões de cidadãos italianos no RaidForums. O autor alegou ter captado esses dados no ano de 2021 e que algumas das vulnerabilidades ainda estão abertas e não divulgadas, mas não estão à venda. Em 13 de junho de 2021, o autor informou que os

dados foram vendidos a uma parte não revelada, grande parte dos dados de vacinação eram pertencentes a indivíduos na região do Lazio.

A Itália tem consciência desses perigos e tem melhorado sua velocidade de resposta contra ataques cibernéticos. Segundo HSS (2021), no dia 3 de agosto de 2021, as autoridades da região de Lazio informaram que os serviços de marcação de consultas seriam restabelecidos nas próximas 72 horas, e no dia 5 de agosto de 2021, o presidente Nicola Zingaretti informou que o agendamento de consultas retornou em outro site, mas isso apenas de forma momentânea, pois um novo site temporário seria lançado até o dia 9 de agosto de 2021, enquanto o site original não fosse recuperado. Segundo o site Ilsole (2021), no fim, o ataque foi solucionado a partir da restauração dos sistemas realizada graças a back-ups robustos que a região de Lazio possuía, priorizando principalmente os serviços de saúde e de vacinação. Ilsole foi confirmado como confiável pelo ANSA IT (Primeira agência de notícias da Itália e uma das primeiras do mundo, criada com a missão de publicar e distribuir informação jornalística). Confira na figura abaixo o nível de confiabilidade dos sites utilizados no ranking do ano de 2019.

Figura 5: Pontuações de confiabilidade na fonte (0-10)



Fonte: Redazione Ansa, 2019.

É necessário ter como verdade que o impacto econômico de um ataque como este não afeta apenas a vítima, também os custos, a infraestrutura do sistema, tornando a dimensão do ataque ainda mais forte, pois atingiu a região como um todo. Outros casos além do

apresentado neste artigo, comprovam essa teoria, como o “Attacchi indiretti[4]” contra uma empresa italiana apresentado por Baldoni (2018), a instituição da província de Cuneo, uma comuna italiana da região do Piemonte, possui uma clientela internacional e sua lista de clientes foi vazada com todas as informações. Os criminosos entraram em contato com os clientes para comunicar que o IBAN (um padrão de identidade internacional de contas bancárias) da empresa foi alterado. Quatro empresas foram contatadas e delas, 3 fizeram pagamentos no valor solicitado, sendo no total US$200.000.

3.3 Como a IA e a Tecnologia Blockchain poderiam ter auxiliado no ataque

A necessidade de investimentos em tecnologia de defesa e segurança cibernética se torna um fator imprescindível para a estabilidade de um país contra ataques cibernéticos. Isso ocorre pois proporciona a proteção da soberania nacional, como foi comprovado anteriormente pelo histórico de ataques que a Itália sofreu até o momento, estados enfrentam frequentemente ameaças de atores, sejam eles estatais ou não estatais, que utilizam ciberataques para desestabilizar um governo principalmente na tentativa de roubo de informações cruciais. Esse investimento pode auxiliar na proteção de infraestruturas críticas como energia, água, transporte e comunicações, sem mencionar que pode proporcionar maior proteção dos ambientes de negócios onde protege a propriedade intelectual da empresa, evitando o roubo de informações e tecnologias importantes ou ainda em desenvolvimento.

O *ransomware* gerou diversas consequências na região, mas a velocidade de resposta foi em torno de 72 horas, esse período de tempo é consideravelmente curto quando se trata de um malware, isso ocorreu pois a resposta ao ataque não conseguiu causar consequências como de se esperado por um *ransomware*. Segundo Nicola Zingarette, Membro da Câmara de Deputados da Itália, em uma publicação em seu facebook reportada no site Ciso Advisor (2021), os dados foram rapidamente migrados para nuvens externas para que fosse possível acessá-las. Uma tecnologia existente que poderia ter sido auxiliadora da região como resposta ao ataque é a mais conhecida como *blockChain*. A tecnologia surgiu sincronizada com a criptomoeda *bitcoin*, seu principal objetivo era armazenar as transações financeiras de todos os usuários da moeda para que não surgissem gastos duplicados (Lucena e Henriques, 2016, p. 1, apud Bovério e Silva, 2018).

Para estudo de viabilidade da utilização de tecnologias de solução e detecção do ataque, a tecnologia blockchain teve seu surgimento em conjunto com a criptomoeda bitcoin.

---

[4] Termo utilizado por Bodoni (2018) como menção a um ataque com alvo ou *Targeted Attack*.

Seu papel é ser fornecedora de segurança e armazenamento na transação de criptomoedas. Diversos casos de ataque de ransomware ocorrem em todo o mundo. Segundo Netti (2024), em média ¾ das empresas italianas relataram um aumento na tentativa de ataque cibernético em relação a ataques contra as estruturas cibernéticas em relação ao ano de 2023 e 12% sofreram os danos desses ataques. Quando o ataque de ransomware ocorre, o dono da máquina pode efetuar um pagamento para resgate dos dados bloqueados e pagamentos são realizados para conseguir a recuperação de forma mais rápida, entretanto os ransomwares proporcionam um ambiente onde essa transação é feita por bitcoins sem possibilidade de rastreio. A tecnologia blockchain auxilia na defesa cibernética contra esse malware a partir do momento em que torna possível o rastreamento dessa transação (Bovério e Silva, 2018).

Essa nova tecnologia pode auxiliar a região nesse caso específico através de diferentes meios. O *blockchain* protege a integridade dos dados, pois realiza utilização de registros distribuídos imutáveis, além de ser possível verificar qualquer tipo de alteração nos arquivos e sinalizar a presença de qualquer tipo de atividade suspeita. Esse método de defesa proporciona um armazenamento seguro de backups, trabalhando principalmente na defesa contra ataques de *ransomware*, são feitos backups críticos para recuperação dos dados mesmo contra ataques que afetam o armazenamento para que não sejam corrompidos (Bovério, Maria Aparecida, and Victor Ayres, 2018).

Sistemas baseados na tecnologia *blockchain*, possuem um controle de acesso à identidade, onde seus sistemas podem aumentar a defesa do acesso e autenticação. Rastreabilidade e Auditoria também são características importantes para atuação da ciberdefesa, pois é possível identificar a origem e a propagação do malware sem causar danos à máquina pois possui uma natureza eficaz contra vulnerabilidade de dados, em síntese, os criminosos criadores do *ransomware* não conseguem atingir todas as infraestruturas de apenas uma só vez, já que os sistemas estão descentralizados (Bovério, Maria Aparecida, and Victor Ayres, 2018).

Outra tecnologia proporcionadora de aumento na defesa cibernética em uma região é conhecida como IA. Podendo proporcionar uma análise comportamental através de monitoramento dos sistemas, a IA identifica padrões incomuns na rede relacionados a atividades maliciosas, além de ser possível detectar problemas ou erros ao acessar arquivos, por ser possível a aprendizagem automática, a Inteligência Artificial pode ser treinada para reconhecer malwares através de uma análise de dados históricos acontecidos no passado, verificando a relação com algum acontecimento recente, referente à plataforma que está sendo utilizada (Romar, 2022).

Segundo Abbass (2021), a inteligência artificial (IA) ainda não tem sua total definição, entretanto pode ser caracterizada como um sistema que irá criar algo similar à mente humana indo além da programação, pois o sistema é preparado para aprender e pensar de forma autônoma. A IA em uma forte ação de detecção de ransomware através de uma seleção de recursos de algoritmos de aprendizagem ou aprendizado de máquina que é treinada através de um processo estruturado que será descrito no presente artigo (Romar, 2022).

A inteligência artificial pode ser utilizada para criar algoritmos automáticos de resposta contra ataques cibernéticos, além da identificação, os algarismos também podem responder diretamente contra o malware, isolando as áreas afetadas e iniciando a recuperação dos dados perdidos. Mesmo que o *ransomware* possa se camuflar através de uma variante desconhecida pela maioria das máquinas, a IA pode realizar uma análise heurística, ou seja, uma análise que visa aumentar a detecção de novas ameaças que podem evoluir constantemente (Romar, 2022).

Essa tecnologia alinha-se diretamente com os objetivos traçados dentro das relações internacionais cibernéticas pois tem seu âmbito de atuação nos campos de ciberdefesa e cibersegurança. A Inteligência Artificial proporciona extrema proteção de infraestruturas críticas que são vitais para a soberania e segurança nacional, além disso, governos e organizações internacionais podem desenvolver políticas tendo a IA como base de detecção, prevenção e resposta contra ataques de *ransomware*, auxiliando também na criação de sistemas capazes de resistir a ataques e se recuperar rapidamente. Esses benefícios proporcionam uma estruturação na soberania do país de forma estável pois os torna preparados contra diferentes tipos de ataques cibernéticos.

4 CONSIDERAÇÕES FINAIS

Qual a importância de investimento em ciberdefesa e cibersegurança para a Itália? A resposta se delimita a partir do momento em que a tecnologia evolui, o ciberespaço se tornou um novo contexto para ataques cibernéticos onde os países utilizam para impor seu poder, disputar hegemonia, obter informações cruciais ou até mesmo apenas atrapalhar algum processo estatal. Ciente disso, a Itália tem investido em estratégias de defesa para possíveis ataques.

Sua execução ocorreu no domingo, 1º de agosto, direcionando-se ao Centro de Elaboração de Dados (CED) da Região do Lazio, resultando também na desativação dos

portais da Lazio Health e da rede de vacinação. Este evento marca o ponto inicial das investigações conduzidas pela polícia postal em colaboração com a Procuradoria de Roma. Até o ano de 2024, não foram encontrados artigos referentes à área geográfica de proveniência do malware que comprometeu os servidores regionais. Intensivas diligências estavam em andamento, conduzidas pelos Correios, em coordenação com o Ministério Público de Roma para identificação dos responsáveis, mas foram finalizadas sem identificação divulgada. Durante o ataque, a região se pronunciou sempre que possível para dissolver a preocupação dos habitantes referente ao ataque.

Segundo a porta-voz da Comissão Europeia do ano de 2021, Sonya Gospodinova, o sistema de saúde, por ser uma das áreas do governo em processo de digitalização, se torna um meio suscetível a ataques cibernéticos, especialmente em um momento tão problemático como o período do Covid-19. A então porta-voz deixa claro em sua fala durante a conferência de imprensa em Bruxelas, em 2021, que cada vez mais esse setor tem sofrido ataques. Isso deixa evidente o quanto a Itália precisa investir em tecnologia de defesa (Ilsole24ore, 2021).

Segundo Alessio D'Amato, conselheiro de saúde da região do Lazio, as funções para novas reservas de vacinas foram restabelecidas dentro de 72 horas. O malware pode ser identificado como um *Crypto-ransomware*, pois ocorreu perda de acesso de dados após os sistemas de TI serem afetados. Segundo o site Ilsole (2021) o ataque teria vindo da Alemanha, mas os motivos pelos quais o país promoveu o ataque é desconhecido, entretanto, podem ser destacados através de diversos meios como por exemplo: coleta de informação, pois o Sistema Internacional se encontrava em um novo contexto com a produção de vacinas vindas de todos os países ou até mesmo por simples demonstração de poder. O *ransomware* gerou impacto, pois se trata de um ataque com danos à rede informática da região causando descontrole dos serviços prestados a empresas privadas, assim como o sistema informático de saúde dedicado à vacinação contra a COVID-19 (Ilsole, 2021).

Casos como o analisado no presente artigo destacam a importância de investimento em segurança e defesa cibernética para um país, pois o mundo está em constante evolução dentro do ciberespaço, isso é destacado a partir do momento em que mesmo os investimentos atuais realizados pela Itália para cibersegurança e ciberdefesa, novos ataques podem ocorrer, pois sempre estão em evolução para conseguir alcançar seu objetivo. Para que seus efeitos não sejam tão graves, ou até mais, comparados ao ocorrido na região de Lazio, é necessário a estruturação e investimento do governo na criação de estratégias de proteção dentro do ciberespaço para impedir que dados sigilosos sejam criptografados ou até mesmo roubados. Esse objetivo deve ser alcançado através de diversas metas como a proteção de infraestrutura

crítica com a utilização de inteligência artificial e tecnologia *blockchain* apresentadas no artigo, pois o ataque paralisou serviços essenciais como sistemas de saúde, causando consequências também na sociedade. Outros riscos como o custo de um ataque, por ser exorbitante por causa de resgates, recuperações de dados e sistemas e prejuízos operacionais também devem ser considerados.

Os governos e instituições públicas concentram uma quantidade enorme de dados em seus sistemas. Proteger esses dados é fundamental para que não ocorram violações de privacidade. Dispor de planos para a recuperação desses dados também é essencial, pois permite que as organizações não sofram tanto. A inteligência artificial poderia ter sido de grande utilização em diversas etapas do ataque. Referente à detecção e à prevenção de ameaças, a IA pode ser capaz de monitorar continuamente o tráfego da rede, assim como os computadores e usuários para que seja possível detectar padrões de possíveis ataques cibernéticos. Além disso, esses sistemas podem automatizar a resposta inicial do ataque isolando as máquinas comprometidas, bloqueando o tráfego. Outra tecnologia mencionada foi a *Blockchain* que pode ser utilizada para a gestão de identidade descentralizada. Isso significa a existência de uma autenticação e controle de acesso proporcionando que apenas usuários autorizados específicos possam utilizar sistemas sensíveis. Também é possível proteger os dados de forma mais eficaz, devido à utilização de registros distribuídos imutáveis que verificam e alertam qualquer tipo de alteração nos arquivos caso ocorra alguma atividade suspeita.

REFERÊNCIAS

Abbass, Hussein. "**What is artificial intelligence?.**" IEEE Transactions on Artificial Intelligence 2.2 (2021): 94-95.

Alison, Aurosa. "**Cos’ è il Cyberspazio.**", 2015.

Bleepingcomputer. “**LockBit ransomware recruiting insiders to breach corporate networks**” Bleepingcomputer, 2021. https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/. Acesso em 14 de março, 2024

Baldoni, Roberto, et al. "**Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici.**" (2018): 1-226.

Bestr.it. "**Cybersecurity National Laboratory - CINI | Bestr.**" Bestr.it, 2015, https://bestr.it/organization/show/149?ln=it#:~:text=Il%20CINI%20 . Acesso em 5 de maio, 2024.

Bovério, Maria Aparecida, e Silva, Victor Ayres Francisco. "**Blockchain: uma tecnologia além da criptomoeda virtual.**" Revista Interface Tecnológica 15.1 (2018): 109-121.

BleepingComputer. "**LockBit ransomware recruiting insiders to breach corporate networks**". 2021. https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/. Acesso em 15 de fev. 2024

Cisoadvisor. "**Ataque de Ransomware Cresce 20% No Brasil; País Já é O 6o No Ranking.**" Cisoadvisor.com.br, 2020, www.cisoadvisor.com.br/ataque-de-ransomware-cresce-20-no-brasil-pais-ja-e-o-6o-ranking/. Acesso 12 de nov. 2023.

CINI. "**Mission - Cybersecurity National Lab.**" Cybersecurity National Lab, 3 Nov. 2023, cybersecnatlab.it/chi-siamo/mission/#:~:text=Il%20CINI%20Cybersecurity%20National%20Lab,su%20tutto%20il%20territorio%20nazionale. Acesso em 5 de jan. 2024.

Ciso Advisor, "**Ataque de ransomware cresce 20% no Brasil; país já é o 6o no ranking**". Cisoadvisor.com.br. Publicado em 2020. Acesso em 4 de setembro, 2024. https://www.cisoadvisor.com.br/ataque-de-ransomware-cresce-20-no-brasil-pais-ja-e-o-6o-ranking/

Ciso Advisor "**Itália: sistema de suporte à vacinação é alvo de ransomware. Cisoadvisor.com.br**". Publicado em 2021. Acesso em 4 de setembro, 2024.

https://www.cisoadvisor.com.br/italia-sistema-de-suporte-a-vacinacao-atingido-por-ransomware/

Ciso Advisor. “**Quem Somos | CISO Advisor.**” Cisoadvisor.com.br, 2018, www.cisoadvisor.com.br/quem-somos/. Acesso em 1 de fev. 2024.

CNN. “**Hackers block Italian Covid-19 vaccination booking system in ‘most serious cyberattack ever**’”, 2021. https://edition.cnn.com/2021/08/02/business/italy-hackers-covid-vaccine-intl/index.html. Acesso em 02 de fev. 2024

CUN - Consiglio Universitario Nazionale. “**ELENCO DEI SETTORI SCIENTIFICO-DISCIPLINARI**” https://www.cun.it/uploads/storico/settori_scientifico_disciplinari_english.pdf. Acesso em 3 de fev. 2024

FRANK, Daniel. “**Cybereason vs. RansomEXX Ransomware**”. 2021. https://www.cybereason.com/blog/research/cybereason-vs.-ransomexx-ransomware. Acesso em 11 de jan. 2024

HASSAN, Nihad A. "**Perícia forense digital**". Traduzido por Aldir Coelho Corrêa da Silva. São Paulo: Novatec Editora Ltda, 2019.

HSS Cybersecurity Program. “**Ransomware Attack on COVID-19 Vaccination Registration Portal in Italy's Lazio Region Possibly Involved Two Ransomware Variants (RansomEXX and LockBit2.0)**”, 2021.

Ilsole. “**Attacco Hacker Alla Regione Lazio, Indaga Anche l’Antiterrorismo - Il Sole 24 ORE.**” Ilsole24ore.com, 2021, amp24.ilsole24ore.com/pagina/AE1Wmga. Acesso em 13 de ago. 2023.

Lakhan, Abdullah, et al. "**RBEF: ransomware efficient public blockchain framework for digital healthcare application.**" Sensors 23.11 (2023): 5256.

Lindsay, J.R., 2013. “**Stuxnet and the Limits of Cyber Warfare**”. Secur. Stud. 22, 365–404.

Villar-Lopes, Gills Vilar. "**Relações internacionais cibernéticas (CiberRI): uma defesa acadêmica a partir dos estudos de segurança internacional.**" (2016).

Villar-Lopes, Gills. “**Relações Internacionais cibernéticas (CiberRI): o impacto dos Estudos Estratégicos sobre o ciberespaço nas Relações Internacionais**”. Congreso Latinoamericano de Ciência Política. Vol. 9. 2017.

LUCENA, Antônio Unias de; HENRIQUES, Marco Aurélio Amaral. “**Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum”.** In: IX Encontro de Alunos e Docentes do DCA/FEEC/UNICAMP, 9, 29-30 de setembro, Campinas, São Paulo, 2016. Disponível em: <http://www.fee.unicamp.br/sites/default/files/departamentos/dca/eadca/eadcaix/artigos/lucena_henriques.pdf>. Acesso em 6 de nov. 2023.

Matassa, Manfredi. "**Una strategia nazionale a difesa del cyberspazio.**" PA Persona e Amministrazione 11.2 (2022): 625-654.

Marrone, Alessandro, Ester Sabatino, and Ottavia Credi. "**Italy and Cyber Defence by Alessandro Marrone, Ester Sabatino and Ottavia Credi.**" DOCUMENTO IAI 21 ISSN 2280-6164. 2021

Netti, Enrico. “**Cybersecurity, Record per Il Mercato Italiano: Spesa a 2,15 Miliardi.**” Il Sole 24 ORE, 23 Fev. 2024, www.ilsole24ore.com/art/cybersecurity-record-il-mercato-italiano-spesa-215-miliardi-AFzaFdnC?refresh_ce=1. Acesso em 5 de fev. 2024.

Pimentel, Eduardo, Cabrera, e Forte. "**Ransomware: do surgimento aos ataques “as a service”.**" FatecSeg-Congresso de Segurança da Informação. 2021.

Redazione Ansa. “**Rapporto Reuters, l’ANSA Prima in Italia per Affidabilità.**” Ansa.it, ANSA, 2019,

www.ansa.it/amp/sito/notizie/politica/2019/06/12/rapporto-reuters-lansa-prima-in-italia-per-affidabilita_ec002e20-be2d-447c-9244-854907918e21.html. Acesso em 12 de nov. 2023.

Romar, Carlos Eduardo Chagas. "**Estudo de métodos de detecção de ransomware utilizando inteligência artificial.**" (2022).

Robert K.yin. "**Estudo de Caso, planejamento e métodos**". (2001)

Saisse, Renan Cabral. "**Ransomware.**" *Revista Eletrônica Direito & TI* 1.6 (2016): 14-14.

Santos, Mário A. "**O quinto domínio como palco da rivalidade entre China e EUA no século XXI.**" II Seminário Discente de Ciência Política da UFPR (SDCP). 2021.

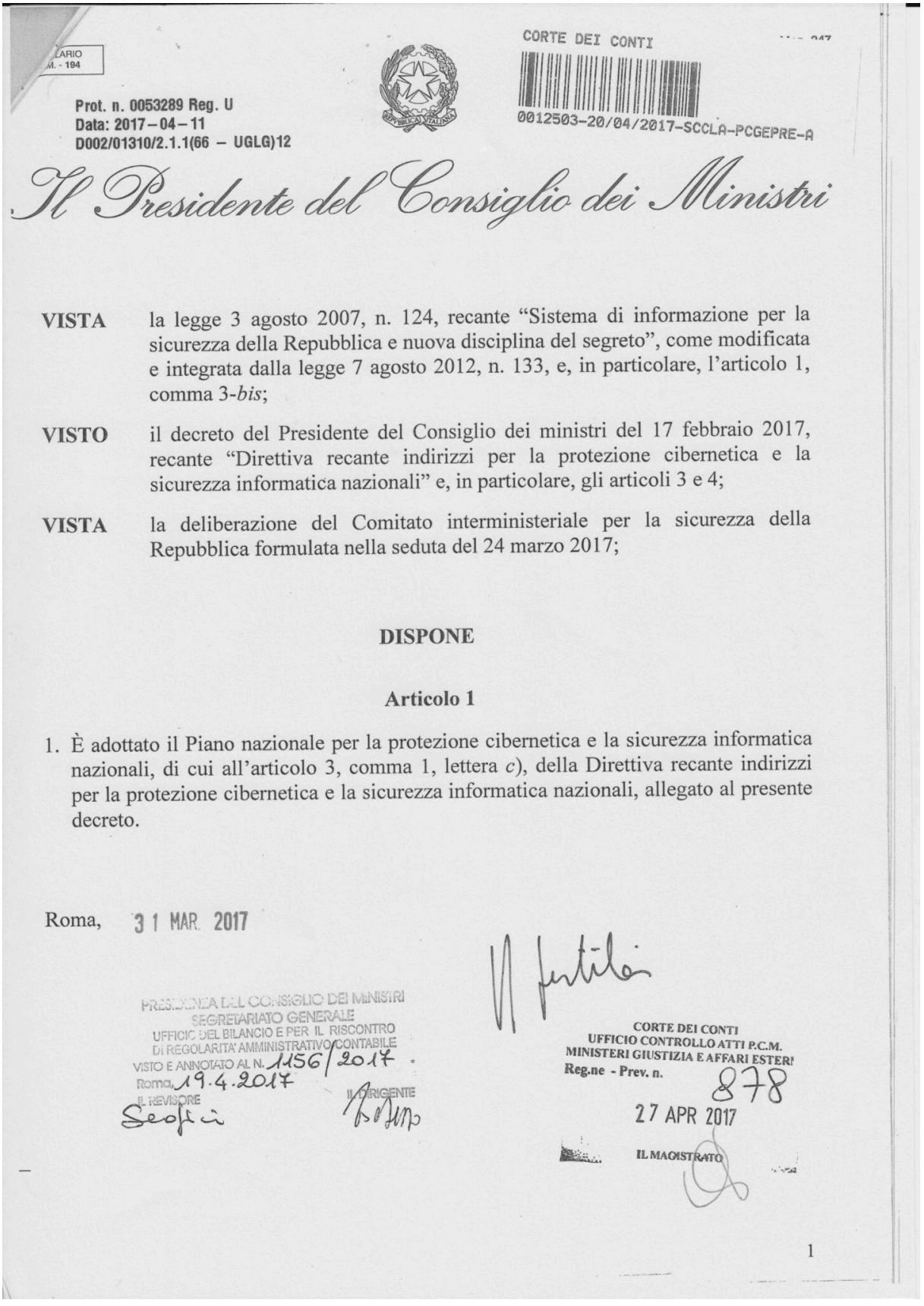
Sharma, Pawankumar, Bibhu Dash, and Meraj Farheen Ansari. "**Anti-phishing techniques–a review of Cyber Defense Mechanisms.**" International Journal of Advanced Research in Computer and Communication Engineering ISO 3297 (2022): 2007.

Silveri, Paolo "**Adozione Del Piano Nazionale per La Protezione Cibernetica E La Sicurezza Informatica.**" Www.governo.it, 31 May 2017, www.governo.it/it/articolo/adozione-del-piano-nazionale-la-protezione-cibernetica-e-la-sicurezza-informatica/7525. Acesso em 12 de nov. 2023.

Souza, Camila Pereira Cavalcanti. "**O uso de criptomoedas em ataques de ransomware: uma perspectiva da sua utilização em ataques cibernéticos**." (2023).

Zetter, Kim. **Countdown to Zero Day - Stuxnet and the Launch of the World's First Digital Weapon.** Crown Publishers, Nova Iorque, 2014

ANEXO A - DOCUMENTOS COMPROBATÓRIOS



LARIO
M. - 194

Prot. n. 0053289 Reg. U
Data: 2017–04–11
D002/01310/2.1.1(66 – UGLG)12

CORTE DEI CONTI
0012503-20/04/2017-SCCLA-PCGEPRE-A

Il Presidente del Consiglio dei Ministri

VISTA la legge 3 agosto 2007, n. 124, recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", come modificata e integrata dalla legge 7 agosto 2012, n. 133, e, in particolare, l'articolo 1, comma 3-*bis*;

VISTO il decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, recante "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" e, in particolare, gli articoli 3 e 4;

VISTA la deliberazione del Comitato interministeriale per la sicurezza della Repubblica formulata nella seduta del 24 marzo 2017;

DISPONE

Articolo 1

1. È adottato il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali, di cui all'articolo 3, comma 1, lettera *c*), della Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, allegato al presente decreto.

Roma, 31 MAR. 2017

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
SEGRETARIATO GENERALE
UFFICIO DEL BILANCIO E PER IL RISCONTRO
DI REGOLARITA' AMMINISTRATIVO-CONTABILE
VISTO E ANNOTATO AL N. 1156/2017
Roma, 19.4.2017
IL REVISORE
Seoffi
IL DIRIGENTE

CORTE DEI CONTI
UFFICIO CONTROLLO ATTI P.C.M.
MINISTERI GIUSTIZIA E AFFARI ESTERI
Reg.ne - Prev. n. 878
27 APR 2017
IL MAGISTRATO

1

ANEXO B - DOCUMENTOS COMPROBATÓRIOS

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 31 MARZO 2017

[Dell'adozione del presente DPCM è stata data comunicazione sulla Gazzetta Ufficiale 31 maggio 2017, n. 125.]

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Vista la legge 3 agosto 2007, n. 124, recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", come modificata dalla legge 7 agosto 2012, n. 133, e, in particolare, l'art. 1, comma 3-bis;

Visto il decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017 , recante "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale" e, in particolare, gli articoli 3 e 4;

Vista la deliberazione del Comitato interministeriale per la sicurezza della Repubblica formulata nella seduta del 24 marzo 2017;

DISPONE

Articolo 1

1. È adottato il **Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali** [PDF 2 MB], di cui all'art. 3, comma 1, lett. a), della Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, allegato al presente decreto.

Roma, 31 marzo 2017

Il Presidente
Gentiloni Silveri

AGRADECIMENTOS

Tenho muito a agradecer às pessoas presentes nos diferentes aspectos da minha vida. Desde meu início de jornada como estudante de Relações Internacionais sempre soube que iriam haver diversas dificuldades, não só com a descoberta de qual área pretendo seguir como Internacionalista, como também devido às mudanças ocorrendo em minha vida, mudar de estado não foi algo fácil, deixar de rever meu amigos antigos e frequentar os lugares que antigamente sempre estava.

Entretanto, mesmo com todas as dificuldades eu me encontrei ao longo do tempo, fiz novas amizades que me proporcionaram momentos incríveis durante todos esses anos de estudo, para essas amizades, gostaria de deixar a minha mais sincera gratidão, obrigado principalmente Lauro Querino, Beatriz Quintanilha, Raquel Bandeira, Rafael Silveira, Andressa Carvalho, João Vitor, Camilly Alves, Evellyn Sudryan, Ilara Ramos, Bianca Aquino e Bianca Flores por todos os momentos vividos. Gostaria de agradecer aos meus pais Michele Rosa e Romildo Faustino Júnior, estou muito feliz por tê-los ao meu lado durante todos os meus anos de vida, vocês são e sempre serão uma parte de mim, espero que nunca esqueçam disso, se eu cheguei até aqui, vocês também tem uma parte de responsabilidade por isso. Além disso, aos meus avós eu agradeço por fazerem parte da minha criação.

Referente ao meu desenvolvimento acadêmico, gostaria de agradecer aos meus professores presentes nessa banca por todos os ensinamentos, em especial as professoras Thays Felipe David de Oliveira e Lucila Gabriella Maciel Carneiro Vilhena. Lucila, a senhora me ajudou a encontrar uma área dentro das relações na qual me identifico profissionalmente, graças aos seus ensinamentos evoluí dentro do mercado de trabalho, Comércio Exterior é uma das minhas paixões dentro das Relações Internacionais. Thays, não tenho palavras para expressar o quanto eu sou grato por tudo, desde a primeira banca no Congresso de Relações Internacionais eu soube que não podia deixar de criar esse *networking*, me admiro com todo o seu conhecimento e espero um dia me tornar ao menos metade de quem você é hoje, muito obrigado por todo o auxílio para o desenvolvimento deste artigo e também agradeço pois sem você não teria conhecido a área de cibersegurança e ciberdefesa, que é a minha área de pesquisa sendo um Internacionalista. Ao professor Filipe Reis Melo, meus agradecimentos por toda a disponibilidade, paciência e dedicação como meu orientador, sem o senhor não conseguiria entregar esse artigo, seu apoio foi essencial para a minha conclusão do curso de uma forma memorável.