SOCIEDADE ALGORITIFICADA: UMA ANÁLISE SOBRE A ESPIONAGEM NA CIBERGUERRA ENTRE A RÚSSIA E UCRÂNIA

Stefan da Silva Toio[1]

RESUMO
Este artigo aborda uma análise crítica da sociedade digital acerca da espionagem na ciberguerra entre Rússia e Ucrânia. Tendo como objetivo entender a possibilidade do sujeito se tornar um alvo perante seu comportamento digital quanto às escolhas de seu passado e presente no campo virtual. Onde, em meio a vigilância digital é visto como um composto numérico e lógico, sem ser levado em conta o fator humano nas tomadas de decisões. Visto que essa pesquisa é baseada através de uma metodologia bibliográfica da qual é realizada uma análise da sociedade contemporâneo totalmente imersivo ao mundo virtual, em conjunto de análise e estudo de caso na guerra estruturado em duas situações: ataque aéreo no teatro de Mariupol e o míssil lançado em um prédio residencial em Kiev. Comparando a análise bibliográfica, estudo sobre ciberguerra e mísseis lançados na Ucrânia. Assim, acaba relacionando que há uma ligação em ambos os fatos, com estruturas discursivas embasadas em cima de suas hipóteses sem elenca-los diretamente, mas relacioná-los sobre resultados e conjunturas considerativas finais, seguindo um pressuposto linear de pesquisa. Essa análise crítica compreende que a sociedade se encontra em perigo através seu próprio comportamento virtual, onde acaba se tornando um alvo móvel sem perceber, pois se tornou totalmente imersivo ao mundo digital, sua integração total à cibernética lhe deixa vulnerável e exposto mediante a uma espionagem e vigilância digital, onde tem como sua privacidade violada e suas informações sendo utilizadas à própria pessoa, fazendo a sociedade se transformar na inimiga de si mesma.

Palavras-chave: Algoritmo. Ciberguerra. Espionagem. Guerra da Ucrânia. Vigilância Digital.

1 INTRODUÇÃO

A sociedade digital expõe seus dados na rede, são coletadas informações de todas as colocações de privacidade no mundo virtual, até mesmo quando não se está inserido diretamente, apenas por estar próximo de uma câmera ou conversar perto de um celular, estão sendo capturados os informativos pessoais para um mundo virtual. Esses dados são compostos binários, estruturas numéricas que são analisadas logicamente, apenas levando em conta os dados e não o fator humano e o impacto que essa lógica se estrutura na sociedade.

[1] Bacharel em Publicidade e Propaganda, possui MBA em Conectividade Total e MBA em Segurança da Informação pela Descomplica, especialização em Filosofia pela Facuminas, especialização em Neuropsicologia Clínica pela UniAmérica, especialização em Teoria da Literatura e Produção Textual pela Faculdade Focus, especialização em Coolhunting pela Faculdades Metropolitanas Unidas. stefantoio@gmail.com

Com isso, esse estudo vem a buscar compreender os parâmetros e hipóteses das ações de espionagem perante a um momento de ciberguerra. Que podem transformar a sociedade como um todo em um campo de guerra, onde o sujeito é um alvo em consequência de seus atos no mundo virtual, e seu comportamento é analisado de maneira lógica dentro do padrão que identifica a possibilidade da existência de um membro hostil na sociedade. Assim, se analisou a ciberguerra entre Rússia e Ucrânia em três aspectos: primeira desenvolvendo-se com teóricos que trazem o problema da relação entre sociedade e tecnologia; a segunda constitui-se na ciberguerra entre os dos países antes e durante o conflito de artilharia; em terceiro é realizado o estudo de casos de duas ações, onde a primeira é o ataque aéreo no teatro de Mariupol, e a segunda é o míssil lançado em um prédio residência em Kiev. E através desta análise, sintetizar os fatos com a análise bibliográfica para se compreender os perigos da vigilância digital na possibilidade de utilizar as informações contra a própria sociedade.

Logo, o objetivo da pesquisa visa trazer a comparação entre os perigos da sociedade quanto a sua imersão digital e privacidade sendo utilizada de maneira lógica em cima das emoções do sujeito. Verificando que ações no mundo virtual podem transformar o sujeito em um alvo sem nem mesmo ele perceber. Onde é parte de uma estrutura baseada em algoritmos que estruturam a quantificação[2] do comportamento da sociedade, sem levar em conta suas emoções, as sensações são observadas analiticamente de maneira genérica para se construir um perfil digital com fins de estabelecer uma zona de controle, embasada em suas vontades virtualizadas.

---

[2] A colocação desenvolvida aqui e no artigo como um todo, constitui-se em relação à quantificação que refere-se ao reducionismo da produção de dados computacionais, o que confere na formação numérica da informação, pois o dado é uma sequência de símbolos quantificados, uma informação só pode ser armazenada em um computador se forem quantificadas, isto é, reduzidas. Assim como também essa termologia explica tem foco conotativo acerca do volume de dados estruturados com base quantitativa, sob denotação de quantidade. O que confere e suma formação similar e análoga nas próximas premissas levantadas durante o artigo - quantificado e quantificar.

2 DESENVOLVIMENTO

2.1 ALGORÍTMO SUBJETIVO: AUTOMATIZAÇÃO SOCIAL

A sociedade é completamente integrada a estrutura algorítmica de ser. Os dados, informações, o binarismo tecnológico estão penetrados em sua reação biológica, composições informacionais que trazem formas de mensagens desejadas para manter uma relação mais próxima com o código. E Acaba fomentando a vontade de permanecer na rede, onde acredita controlar os dados e é controlado ao mesmo tempo pela arquitetura sistêmica computacional. Assim, o binarismo tecnológico constitui a ser sua realidade e imaginário construindo a maneira de estar sob uma rotina vivida em pacotes de dados transmitidos de maneira lógica. O eu é quantificado e analisado logicamente sem levar em consideração seus sentimentos, são fragmentos de sensações simuladas construídas de maneira numérica para moldar o comportamento a seu favor. (SADIN, 2015, p. 133-155)

Logo, a vida numérica se baseia em ações cotidianas proferidas pelas vontades construídas em forma de feedback, onde o comportamento é uma equação algorítmica, estruturado no binarismo tecnológico que tem como objetivo desenvolver uma forma lógica de ser. (SADIN, 2015, p.62-65). Assim, dentro do mundo digital a sociedade vem a vigiar-se, controla as próprias sistemáticas cotidianas e sente pressionada a não errar, pois ela acaba desenvolvendo uma autovigilância. Fazendo-se viver no panóptico digital porque seus dados são passados para empresas, suas postagens são analisadas e toda intimidade se torna pública. Assim, a sociedade é distante, vigilante virtualmente para formar seu próprio autocontrole. (HAN, 2014, p.33-35)

Com isso, se pode perceber que a vigilância virtual tem sua própria dimensão de localização, tratando a experiência como objeto quantificado e trabalhado logicamente para se chegar a denominadores comuns, buscando a precisão baseada em sistemáticas de protocolos computacionais sobre o comportamento numérico. Onde os humanos são as análises de informações de outros humanos, e essa observação se torna recursiva e ninguém escapa das próprias ações analíticas. (SADIN, 2015, p.179-170)

Nisto, entra o papel das inteligências artificiais que ajudam no processo analítico, trabalhando com grande volume de informações, realizando funções comparativas em estruturas algorítmicas, contribuindo para o recorte e discriminação dos dados. Estes dados são efeitos comportamentais e informações pessoais, pois são levantados atributos das pessoas de maneira racional. Onde os objetos e as palavras são observadas de maneira terceirizada por uma inteligência que não leva em conta o fator humano imprevisível, pois tem apenas como fundamento analisar suas funções numéricas com precisão. (SADIN, 2020, p. 180-184)

Então se pode entender que a precisão tecnológica faz com que se construa o desempenho social desenvolvido em um novo símbolo da utilidade humana sem levar em conta sua dignidade, tendo com objetivo apenas satisfazer os objetivos egoístas através de sua intersubjetividade racionalizada, condicionando os valores pessoais se transformarem em performance através da base de fatores individualizados. (SADIN, 2020, p.187-189)

Visto que, pode-se perceber dentro da conduta de fatores automatizados dentro do comportamento algorítmico, condiciona-se a uma combinação de fatores dos quais perpassam ao controle e a vigilância. O binarismo comportamental se transforma em expressões ambíguas e todo sujeito pode ser alvo. O controle da ação e reação pessoal perante a sociedade se torna em uma forma libertadora de controlar a liberdade, por mais que possa parecer paradoxal tal expressão, é a forma de se manter vigilante. Os atos são contabilizados, havendo análise acerca da performance do bom comportamento dentro do modelo padrão de estar virtualmente aceitável, onde a vigilância e o controle são chamados de cuidado, como uma proteção do inimigo de si próprio. (SADIN, 2020, p. 217-221)

Uma vez que, o a sociedade é código, o código é estruturado e moldado conforme as afirmações do sentido de bom cidadão são estabelecidas dentro de uma arquitetura algorítmica, onde o sujeito é adestrado sob sua maneira de estar, pois seu comportamento é administrado como um dado analítico que vai se

ajustando conforme o que convém ao administrador, parecendo um totalitarismo invisível reagindo por trás de suas condutas. Isso acontece porque a [...]

> [...] administração comportamento automatizado tenta generalizar o princípio de uma internalização dos preceitos estimados como "fundamental" para que, como cercas elétricas que delimitam determinados espaços, sejam enviadas descargas aos elementos do rebanho que se extraviam e sair do perímetro planejado, descuidada ou voluntariamente. A arquitetura da matriz é suficiente por si só conter toda a inconstância divergente. (SADIN, 2020, p.222)

Por fim se compreende que há uma estrutura administrativa dos comportamentos humanos, baseadas na forma digital de ser, que analisa os dados da sociedade com objetivo de quantificar sua forma de ser, o embasamento generalizado de seu comportamento é levado em conta, com fins de estabelecer uma sociedade codificada e automatizada dentro da natureza vigilante.

2.2 INTELIGÊNCIA VIGILANTE

Após analisar o comportamento da sociedade com campo digital, onde o da mesma é vigiada e analisada logicamente. Percebe-se que dentro desta premissa cabe compreender os parâmetros da espionagem quanto às óticas colocadas acerca da vigilância. Logo, se tem como base de compreensão sobre a espionagem, e pode-se encontrar as colocações das quais PURNELL (2021) explica que, o espião age de maneira oculta sobre coisas das quais as pessoas não dão importância, onde são reveladas as verdadeiras informações e perfis psicológicos profundos. Tendo como objetivo tomar forma dentro das outras tomadas de formas, vigiando o vigilante, não estando escondido e nem amostra de qualquer sistema, mas fazendo parte do sistema como uma pessoa comum que comete erros e acertos com objetivo de não ser notado pelo excesso de perfeição e imperfeição. O papel do espião é fazer parte do cotidiano enquanto as coisas acontecem, durante a vivência e assim se molda, aprende, observa os alvos e chega a determinadas conclusões até o momento de seu ataque de informação.

Assim como também se pode observar a análise de SNOWDEN (2019) colocando que uma agência de inteligência é capaz de armazenar bancos de dados de pessoas, realizando espionagem de maneira geral de todas as estruturas digitais: câmeras, acessos, áudio. Todas as participações cotidianas do ser humano me meio ao campo digital. Todo sujeito pode ser possível alvo e ter todas as informações espionadas e analisadas, pois através de uma determinada conduta passa a ser suspeito e posteriormente inimigo do estado, tendo informações privadas espionadas, sendo observando enquanto possui uma ilusão de privacidade.

Ainda segundo SNOWDEN (2019) os bancos de dados do serviço de inteligência possui grande volume de dados de pessoas que acreditam viver no anonimato, mas apenas fazem parte da sistemática de espionagem, onde aquele que espiona é espionado, aquele que vive de maneira anônima é observado anonimamente. Não tendo onde se esconder, fazendo parte de uma blacklist de inteligência como possível alvo, passando a ter todos os e-mails, escutas telefônicas, dados excluídos, acessos, conversas privadas; sendo analisados em tempo real e fazendo parte do servidor local de inteligência.

Com essa explicação sobre a espionagem, encontra-se a ciberespionagem agindo no cotidiano da sociedade digitalizada. A ciberespionagem tem como função captar informações de companhias, grupos e governos; possuindo informações secretas que compõem o núcleo sistêmico de determinada organização. Tendo como foco obter vantagens acerca de determinadas concorrências, onde o seu fundamento se baseia a compreender o sistema de existência do todo como uma competição. (BAPNA; CHEN; HUA, 2015, p.67-69)

Sua ação de competitividade além de encontrar pontos fracos do concorrente, visa compreender seus segredos e os conceitos dos quais permeiam seus caminhos futuros, isto é, entender para onde vão suas direções e assim conseguir chegar primeiro que a concorrência. Visto que toda e qualquer informação protegida de qualquer lugar possa trazer vantagem. (BAPNA; CHEN; HUA, 2015, p.67-69)

Com essas premissas sobre espionagem e posteriormente sobre ciberespionagem. Compreende-se em uma gama geral dessas explicações que a espionagem tem como objetivo obter vantagem sobre seus alvos, infiltrando-se dentro do cotidiano através do comportamento rotineiro, onde aos poucos mantém uma base informações para estar a frente de qualquer competição informativa.

2.2.1 Ciberguerra entre Rússia e Ucrânia

Após o entendimento explicado nos assuntos anteriores sobre algoritmo subjetivo que traz a questão da automatização social, trazendo ênfase na vigilância da sociedade no mundo digital, que tem seu comportamento analisado logicamente com base de estudo de algoritmos. Dentro destas fundamentações encontrou-se a espionagem que faz parte desta participação vigilante, tendo como objetivo tirar vantagem e manter uma base de informações sobre os alvos. Pode-se compreender a relação entre automatização social com a espionagem. Assim, este tópico visa trazer observações seguidas das duas premissas levantadas anteriormente, dando ênfase a ciberguerra entre Rússia e Ucrânia, mostrando a base de dados da Kaspersky para demonstrar as elevações de detecções das infecções nos sistemas, demonstrando também o objetivo de cada país em uma guerra cibernética, para se compreender melhor qual o percurso final de cada objetivo derivativo de uma espionagem, levando em conta os alvos apontados.

Com isso, pode-se perceber que segundo KASPERSKY (2022) dentro do período de trinta dias, contando de 1 de março até 30 de março, a Ucrânia sofreu[3] poucos ataques de ransoware – com exceção o dia 21de março onde elevou-se e teve uma queda brusca no dia seguinte – onde a maioria do tipo de ransowares eram Blocker Checks contendo 21% dos ataques deste tipo neste mês. Altos índices de escaneamento de vulnerabilidades por parte do atacante, contendo

[3] Os ataques aqui analisados através da Kaspersky são relatados de maneira geral, sem relatar atacante ou construtor de vírus específico. São colocados para mostra o tipo de vulnerabilidades exploradas dentro do país, segundo as análises colhidas pela Kaspersky. Essa análise serve para observar a Ucrânia e a Rússia.

diversos tipos de escaneamentos, contudo o mais realizado contendo 12% dos escaneamentos foram Exploit.Script.CVE-2021-26855.gen, em segundo lugar exploits voltados à falha do Office, contendo 11% dos escaneamentos. Tendo também ataques de intrusão força bruta Bruteforce.Generic.Rdp.d contendo 32% dos ataques deste tipo, tendo picos altos de ataques em 5 de março e 23 de março. Diferente dos ataques de malware através de sites e download, que se elevaram até o dia 2 de março e tendo uma queda significativa até dia 7 de março, subindo dia 8 de março, após a queda deste dia, obteve uma constância nos ataques, onde o tipo mais utilizado foi Trojan, sendo o Trojan.BAT.Miner.gen contendo 39,13% dos ataques, seguidos do Trojan.Script.Miner.gen possui 30,94% dos ataques. Recebidos também malwares em e-mails com fluxo alto nos dias: 9, 16, 21 e 28; com maioria dos ataques Trojan.MSOffice.Generic no mês, sendo 11,03% dos ataques, seguidos os ataques Trojan-Spy.MSIL.Noon.gen sendo 10,42% das ações gerais. Assim como, os computadores estarem infectados por 15,19% com Trojan.Multi.BroSubsc.gen, elevando-se dia 14 de março, diferente dos vírus que se aplicam em objetos acessáveis contendo 20,6% com DangerousObject.Multi.Generic, com picos em: 5, 13 e 19 de março.

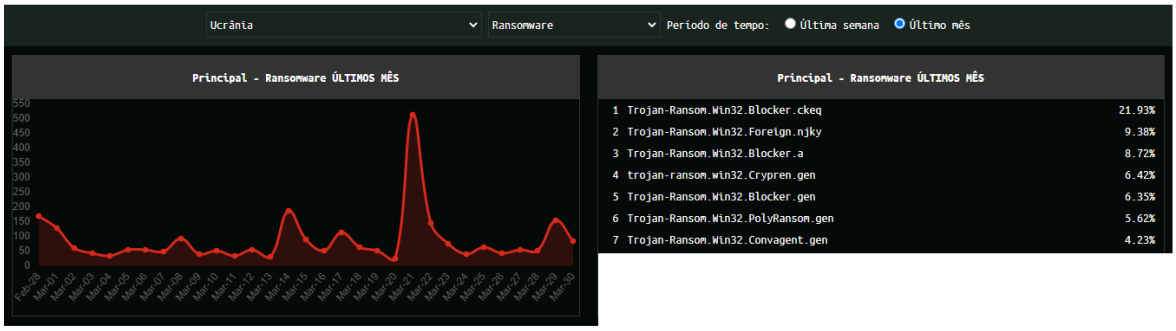

Figura 01 – Escaneamento de Ransoware na Ucrânia.
Fonte: Kaspersky, 2022.

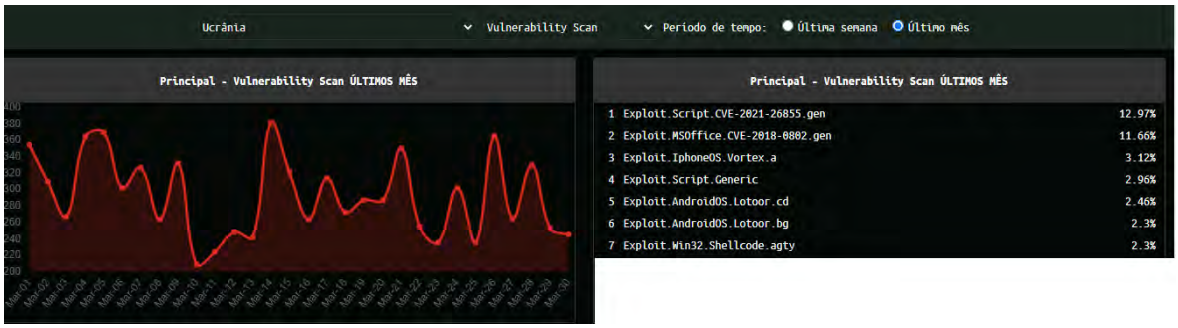

Figura 02 – Escaneamento de Vulnerabilidade na Ucrânia.

Fonte: Kaspersky, 2022.

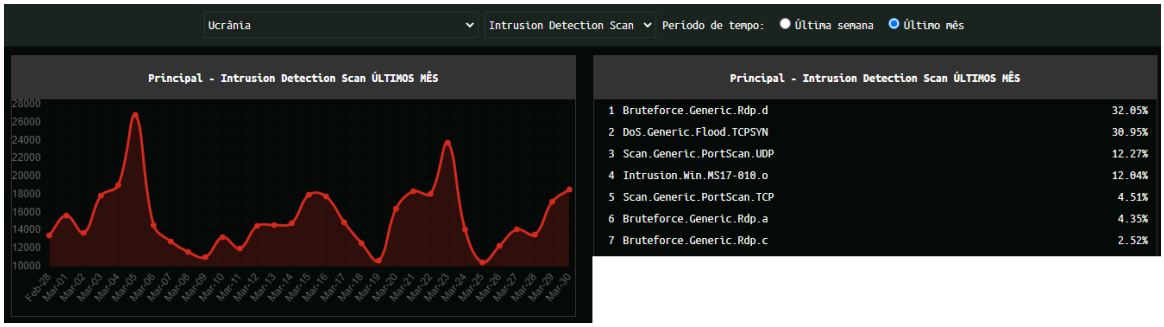

Figura 03 – Escaneamento de Detecção de Intruso na Ucrânia.
Fonte: Kaspersky, 2022.

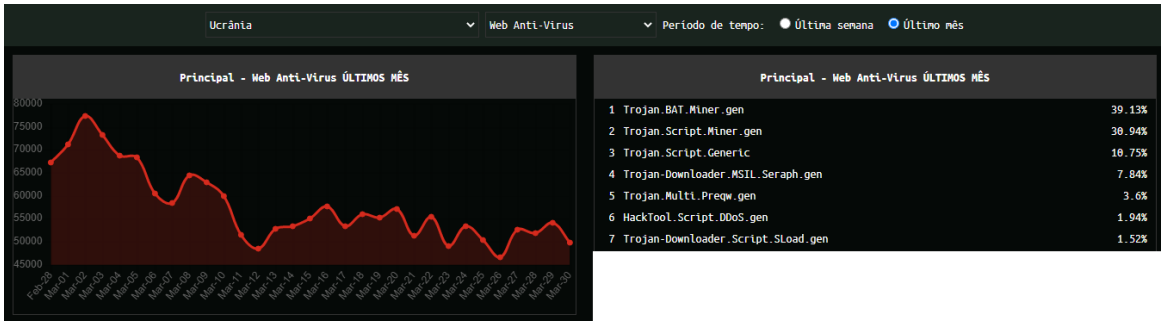

Figura 04 – Escaneamento no Processo de Verificação na Ucrânia.
Fonte: Kaspersky, 2022.

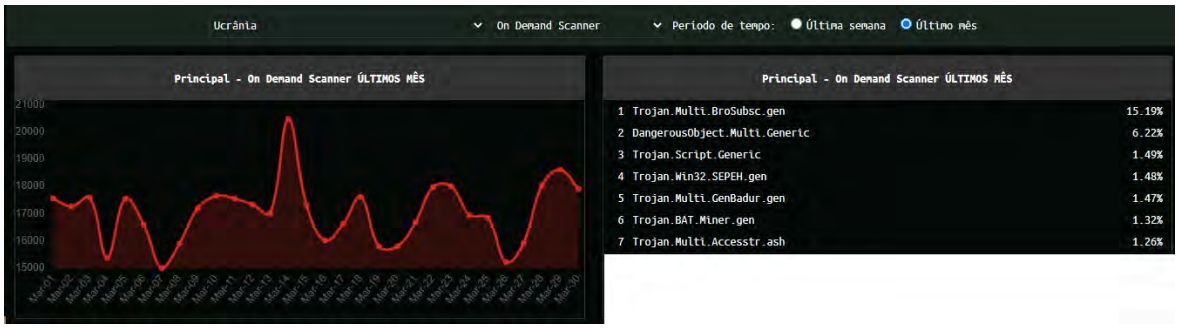

Figura 05 – Escaneamento Sob Demanda na Ucrânia.
Fonte: Kaspersky, 2022.

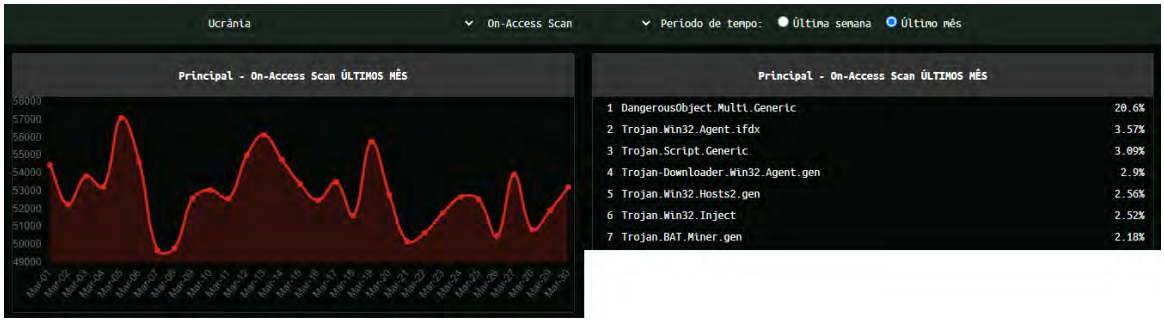

Figura 06 – Escaneamento de Acesso na Ucrânia.
Fonte: Kaspersky, 2022.

Conforme relatado acima segundo KASPERSKY (2022) os ataques são com dinâmicas mais voltadas para escaneamento de vulnerabilidades, trojans infiltrados nos aparelhos, grandes fluxo específicos em tempos específicos para malwares por e-mail e infecção de computadores, em suma grandeza de diversificação, pois elencou poucas taxas de porcentagens em maiorias de ataques, como também grandes taxas de níveis de ataques de força bruta, para invasão. Diferente dos vírus acessáveis que obtiveram dias específicos mas com constância de ataques sofridos. Entretanto, os ataques de ransowares são baixos, comparados aos outros tipos de ataques. Nisto se percebe a mentalidade dos ataques sofridos, com objetivo de infiltração de dados, injeção de captadores de dados, força bruta, malwares para se ter domínio dos dados. Esses ataques proferidos na Ucrânia obtiveram estrutura enfática de invasão e não a total desestabilização sistemática, por mais que possa parecer sob primeiras vias.[4]

Nisto, se pode perceber também que no período do início de guerra em 2022 entre Rússia e Ucrânia, os ataques cibernéticos da Rússia foram utilizados para fins de espionagem. Como também para conseguir observar a resposta do mundo mediante a sua invasão. Utilizando também ataques phishing em autoridades ucranianas e militares poloneses para roubo de dados, e também a Rússia busca ter acesso as informações sobre as decisões dos governos sobre que sansões serão aplicadas, para compreender suas medidas e colocações em futuras negociações. (DAVIES, 2022).

[4] Os ataques inseridos dentro das detecções da Kaspersky na Ucrânia são de cunho geral, sem enfatizar os endereços dos atacantes, focando apenas nos pontos de vulnerabilidades do país.

Em relação aos ciberataques na Ucrânia, Doug Madory da empresa Kentik de observatório da internet, a Ucrânia sofreu ataques cibernéticos dos quais deixaram sua internet desestabilizada, onde foram derrubadas as principais provedoras de internet ucranianas: Ukrtelecom e Triolan. (MARIN, 2022)

Também se pode perceber que os ataques provindo daqueles que apoiam a guerra seguiram a mais de 3.000 ataques DDoS com pico de 275 ataques DDoS e um dia, chegando até mesmo atingir o pico de 100Gbps. Os ataques possuem um repositório de pacotes Node.js e NPM, onde os códigos se mantém atualizando para comportar a Rússia e Bielorrússia. Também houve interrupção dos serviços de satélite Viasat na Europa Central e Oriental, corrompendo o fimware. Mediante aos bloqueios informativos dentro da Rússia, ouve um grande volume de softwares VPN baixados, assim como ferramentas como Signal e Tor, utilizando a tecnologia Snowflake. Houveram também ataques de malwares contra alvos ucranianos, um deles fazia download automaticamente de dados dos alvos, enquanto outro malware chamado CaddyWiper realizava uma limpeza nos sistemas. (WISNIEWSKI, 2022)

Em compensação os ataques provindos para o lado Rússia tiveram outro objetivo. Conforme se pode perceber segundo KASPERSKY (2022), em suma contra partida, onde a Rússia sofreu grande volume[5] de ataque ransoware, elencando 31,64% do Trojan-Ransom.Win32.Blocker.ckeq, com altas elevações de picos, como também se pode perceber as alternâncias de escaneamento de vulnerabilidades com 21,88% de Exploit.MSOffice.CVE-2017-11882.ge seguidas de 14,62% de Exploit.Script.CVE-2021-26855.e. Também se pode verificar picos e constância nessas elevações de detecção de intrusos com cerca de 33,36% de Bruteforce.Generic.Rdp.d, seguidas de 27,21% de Intrusion.Win.MS17-010.o, Diferente das detecções de malware que ao mesmo tempo em que ocorrem essas elevações, elas possuem uma constância, predominando uma linearidade, constituindo um perfil de aplicação de malware e tendo como 76,7% de Trojan.BAT.Miner.gen, diferente da detecção do fluxo de malware em e-mail,

[5] Aqui não leva em consideração apenas o volume, pois ela é proporcional ao tamanho do país, o que se leva em conta são as elevações e as investidas nos tipos ações aplicadas.

demonstrando constância, obtendo um grande nível de fluxo em 21 de março, seguidos em suma maior de 20,96% de Hoax.Script.Scaremail.gen. Se verifica também a grande constância elevada de detecções em objetos nos aparelhos, de maneira constante e em desordenação e contendo 21, 77% de DangerousObject.Multi.Generic; diferente das intrusões com escaneamento nos aparelhos com fluxo de malware padronizados depois de uma modulação inconstante de dinâmica, tendo apenas 14,96% de Trojan.Multi.BroSubsc.gen, pois manteve-se em variação de trojans aplicados.

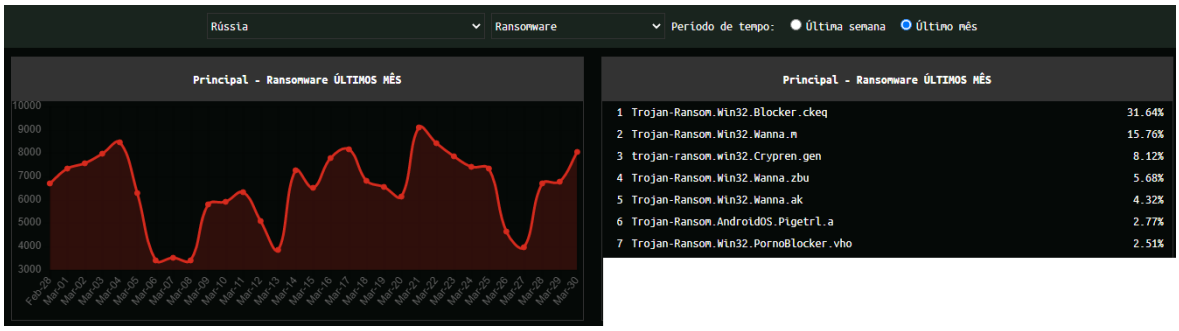

Figura 07 – Escaneamento de Ransoware na Rússia.
Fonte: Kaspersky, 2022.

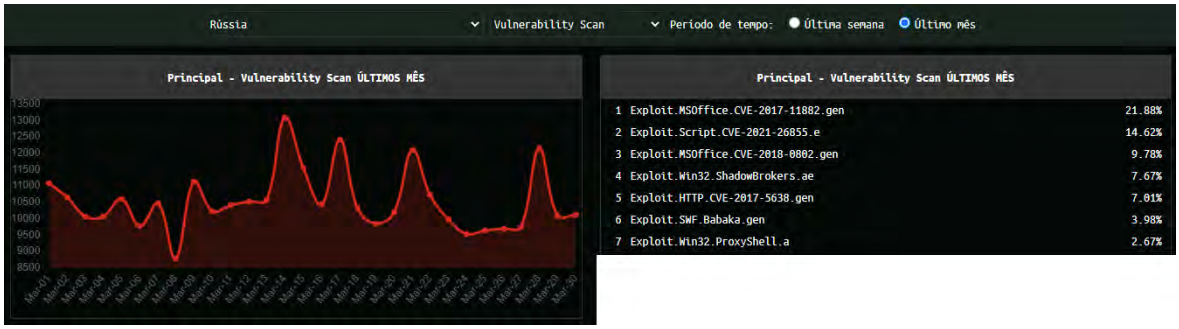

Figura 08 – Escaneamento de Vulnerabilidade na Rússia.
Fonte: Kaspersky, 2022.

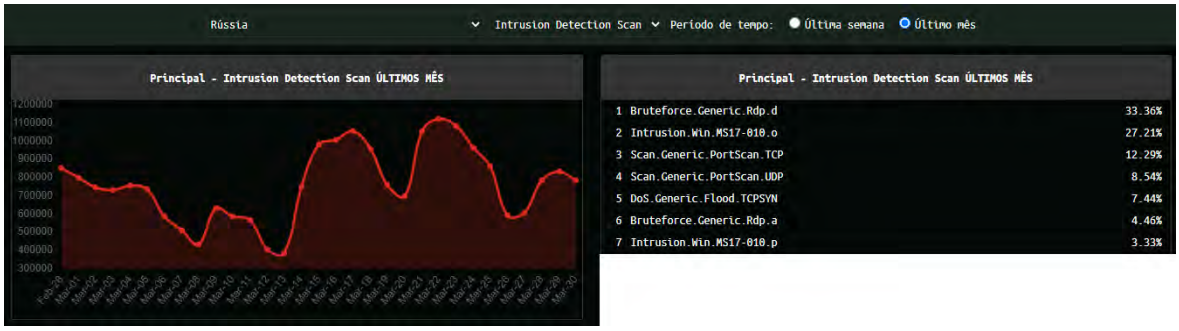

Figura 09 – Escaneamento de Detecção de Intruso na Rússia.
Fonte: Kaspersky, 2022.

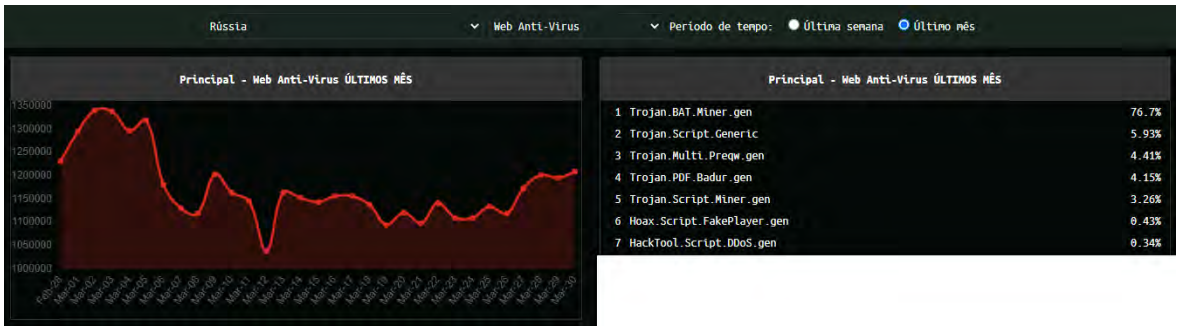

Figura 10 – Escaneamento no Processo de Verificação na Rússia.
Fonte: Kaspersky, 2022.

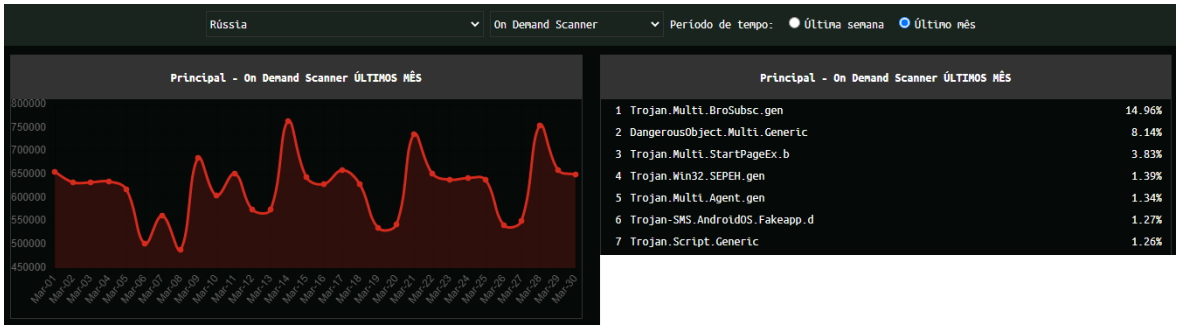

Figura 11 – Escaneamento Sob Demanda na Rússia.
Fonte: Kaspersky, 2022.

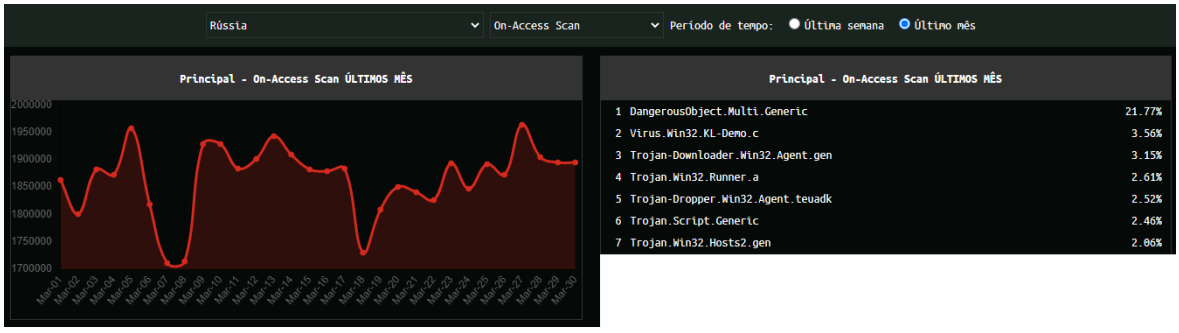

Figura 12 – Escaneamento de Acesso na Rússia.
Fonte: Kaspersky, 2022.

Conforme relatado acima se percebe que segundo KASPERSKY (2022) há uma padronização de ataques, com elevações e picos coordenados, seguidos de constâncias que fazem o papel de fortalecimento da permanência de aplicações, para facilitar as formas de ações em cima do país, com altos carregamentos de reações, como se estivesse sendo ataca com um objetivo específico, em padronizações determinantes das atividades intrusivas seguidas de maneiras conjuntas doutras formas de ações.

Com isso, também se pode entender uma suposta violação de dados no Roskomnadzor, censor de internet do Kremlin. Também se obtiveram ataques que violaram a Transneft, empresa de russa de oleodutos, sendo roubados mais de 79 gigabytes de e-mails, tendo o vazamentos da DDoSecrets. (WISNIEWSKI, 2022). Como também a Ucrânia possui um exército cibernético de voluntários, tendo mais de 300 mil participantes, incluindo: White hats, Black hats e também gangue de ransoware Conti. Enquanto alguns ISPs Ucranianos tinham sido retirados a Starlink acabou dando suporte[6] para a Ucrânia. (BENNETT, 2022)

Como também a Ucrânia neste período de guerra, está com exército de T.I, que se chama IT Army of Ukraine, se comunica pelo Telegram, onde expõe alvos para a realização de ataques cibernéticos, coloca em exposição portas tcp, ip's, sites de diversas companhias e empresas ligadas ao governo russo. Além de alterar os sites russos informando a população russa em um trabalho de contrainformação do qual tenta impedir da Rússia conseguir ter controle da opinião pública através de suas informações estatais. Essas informações incluem imagens da guerra, informativos de jornais de diversas partes do mundo. (IT ARMY OF UKRAINE, 2022)

[6] Diferente do método convencional de internet, a Starlink trabalha com método via sinal diretamente ligado aos satélites, impossibilitando a interrupção de sinal de internet. Além de oferecer o sinal gratuito a Ucrânia, disponibilizou antenas para a população ucraniana. (LERMAN; ZAKRZEWSKI, 2022)

Nisto se pode perceber um volume de ataques cibernéticos provindo dos dois lados da guerra, enquanto a Ucrânia tenta realizar uma mobilização interna dentro da Rússia, além de colapsar seus sistemas e roubar suas informações. A Rússia tenta desestabilizar o sistema da Ucrânia para manter o desenvolvimento de seus ataques, compreendendo alvos e roubar informações da Ucrânia. No meio desta sistemática de guerra se pode perceber também a sociedade digitalizada enquanto atacante e defensor cibernético. Assim como, a base populacional sem compreender que faz parte deste jogo de informações, roubo de dados, sendo espionado, pois integrou-se totalmente ao mundo digital sem perceber as ramificações das quais seu comportamento e registro virtual estariam em jogo.

2.3 ESPIONAGEM DA RÚSSIA NA UCRÂNIA: O INIMIGO DE SI MESMO E OS MÍSSEIS ISOLADOS.

Dentro do cenário colocado acima nos temas e conceitos levantados, se percebe uma ligação entre automatização social, algoritmo subjetivo, vigilância, espionagem, ligados a uma sistemática estratégica de ciberguerra, onde cada país tem seu objetivo definido. Contudo, o enfoque voltado para a espionagem da Rússia nesta estrutura tem seu aporte de ação quanto a mobilização social entre o real e o virtual. Onde seu enfoque se direciona no roubo de dados, derrubada de sistemas, adjunto a isso conseguir informação de possíveis alvos. Assim esta premissa se baseia no levantamento das informações dos temas acima, sobre a demonstração ação vigilante adjunto a espionagem e seus objetivos em uma guerra, onde a sociedade em porto digital acaba se tornando alvo.

Ainda nesta colocação sobre a espionagem da Rússia sobre a Ucrânia, se pode perceber que a Rússia possui o avião espião Tupolev Tu-214R, que foi visto na Síria sendo escoltado por jatos caças Su-39SM, sobrevoando a província de Idlib. O mesmo avião foi descoberto sobrevoando a Ucrânia em 2015, depois foi descoberto em julho de 2016 sobrevoando próximo da fronteira com a Letônia, Estônia e Finlândia. Este avião é enviado para missões de ISR (Intelligence Surveillance e Reconnaissance), ELINT (Eletronic Intelligence) e SIGINT (Signal

Intelligence). Onde intercepta sinais de radares, veículos de combate, aviões e celulares; podendo desenvolver uma ordem eletrônica de batalha, compreendendo quais equipamentos o inimigo utiliza e suas localizações, além de espionar as comunicações por rádio e telefone, podendo ajudar na prevenção dos próximos passos de seus alvos. (GALANTE, 2016)

A Rússia também possui esferas robóticas para espionar zonas de guerra, uma bola robótica contendo microfones e quatro câmeras para se ter uma visão 360 graus, essa esfera robótica é utilizada para missões de espionagem, tendo o nome de Sphera, ela tem 50 metros de distância do dispositivo de comando. Já foram testadas na Síria em 2018, mas ainda não foi vista ao redor da Ucrânia, pois a Rússia levou em conta a participação de ataques digitais, onde está sendo investida a guerra cibernética. (GONÇALVES, 2022)

Logo, a guerra cibernética por parte daquele quem espiona que tem como foco o levantamento de dados e manter a constância vigilância, podendo chegar a determinadas conduções de seus alvo. Entende-se mais claramente a perspectiva da espionagem e suas tecnologias, sob uma análise similar acerca dos dados pessoais no jogo WATCH DOGS 2 (2016), onde em sua introdução demonstra a imersão da sociedade no mundo digital e sua privacidade. Todos os dados são transformados em perfis, trabalhando em rede para constituir sua personalidade virtual, atribuindo a violação da privacidade em prol da segurança, onde todos são observados e tratados conforme se condiciona seu comportamento no mundo virtual[7]:

> Brinquedos estudam nossos filhos, repassando seus hábitos para os fabricantes. Utensílios, painéis e sistemas de segurança transmitem sua vida privada para as empresas. O controle do seu carro e celular pode ser tomado remotamente por qualquer um a qualquer momento. Você pode se achar imune e ignorar os riscos, mas a sua sombra digital já foi comprometida. As empresas de segurança usam algoritmos para monitorar seus hábitos e limitar ou bloquear a cobertura. Planos de saúde preveem se vale a pena tratar o seu câncer. Notícias e resultados de buscas são manipulas para influenciar seu voto, maquinando revoltas sociais em larga escala. Hoje, seus dados valem mais do que sua vida.

[7] A perspectiva atribuída neste artigo se condiciona a compreender a questão dos dados sendo trabalhos para desenvolver um perfil do sujeito, e assim o tornando alvo. Entendendo o viés acerca da privacidade digital para detalhar e sintetizar as ramificações que atribuem ao tema da pesquisa.

> Essa é a nova realidade. Controle é uma ilusão; sumir não é mais uma opção. (WATCH DOGS 2, 2016)

Podendo perceber que os dados e a privacidade estão fragilizados com a sociedade, e nesta ótica se pode perceber que HAN (2014) coloca que a big data[8] é a ferramenta mais poderosa do instrumento psicopolitico, possui uma forma de controle mais integrada, com a perspectiva de 360 graus da vigilância, pois a vigilância não é forçada, ela é convidada a participar da vida social. Os dados fazem parte da ferramenta de dominação, intervindo a psique e modifica a forma da liberdade, a sociedade se entrega livremente aos dados. É convidado a perder a sua liberdade enquanto possui a crença de estar mais livre do que nunca, o condicionante autônomo controlado dentro do próprio cotidiano.

Com isso, se poder perceber que a guerra cibernética e espionagem são aliadas nas suas estruturas comportamentais quanto à dominação do inimigo. Como visto no filme Snowden – Herói ou Traidor, onde coloca uma cena em exposição em que Snowden perguntou as seus colegas de trabalho sobre um carro contendo pessoas dentro, e recebe a resposta de um de seus colegas que a agência possui alguém do serviço de inteligência no local para confirmar o alvo, assim o outro colega olha para trás e balança a cabeça confirmando que não há nenhum agente de inteligência por perto, logo então Snowden se depara com a realidade que aquele alvo é alguém puramente construído em seu perfil cibernético como inimigo, os dados o fizeram assim, o transformaram em alvo móvel através de seu comportamento virtual. Visto que, ele ao observar a tela enxerga o míssil de um drone atingindo o carro, matando todas as pessoas dentro dele, fazendo-o se questionar que a espionagem tecnológica estivesse fazendo da sociedade inimiga de si mesma.[9] (FITZGERALD; STONE, 2016)[10]

---

[8] A colocação de Han se baseia não apenas na vigilância, mas também no grande volume de dados da sociedade, armazenados e utilizados no cotidiano.

[9] Por mais que esse filme se aplique como uma mensagem acerca da espionagem estadunidense, sua visão crítica rege de forma geral quanto a sociedade e sua privacidade no mundo virtual. Desta ótica crítica que se aplica neste artigo, para trazer a compreensão acerca da sociedade e sua total imersão ao mundo digital.

[10] O objetivo da colocação do jogo Watch Dogs 2 e o filmes Snowden – Herói ou Traidor, é com objetivo de tornar mais tácito o que foi elencado em outros tópicos. Facilitando a viabilidade da análise dos casos abordados. O que não torna uma opinião de fato através da literatura, mas a literatura servindo como complemento das bibliografias e os fatos.

Assim, se compreende como os dados podem ser utilizados contra a sociedade, quando aliados à alvos seguidos de constância espionagem. Então se pode perceber nesta perspectiva da sociedade vigiada, espionada e se tornar alvo. Algo do qual está exposto nesta lógica, durante o bombardeiro da Rússia durante a invasão na Ucrânia. Onde atribuía misseis disparados de maneira autônoma e isolada, atingindo civis, sem ligações diretas com a força de resistência e militares. Em zonas não conflitantes em polos do país. O que deixa em dúvida em como a Rússia conseguiu perceber possíveis alvos, e o trabalho de inteligência mediante as informações passadas as ações militares. Como se pode perceber o míssil lançado no Teatro de Mariupol, local que servia como refúgio para mais de mil pessoas, ao lado de fora do prédio estava escrito no chão com letras grandes em Russo a palavra Crianças, com objetivo de informar os russos que era um local de civis. Contudo, após o bombardeio foi realizada uma contagem em aproximadamente 300 mortos. Enquanto o ministro de Relações Exteriores ucraniano acusou a Rússia de crime de guerra, o Ministério da Defesa da Rússia negou que o bombardeio partiu deles, e sem provas acabou culpando o Batalhão de Azov pelo ocorrido, feito com proposto de culpar os russos. Entretanto, já se estima 3 mil civis mortos na cidade com 80% dos edifícios destruídos, segundo a ONG Human Rights Watch (HRW) explicou para The Guardian que a cidade estaria repleta de cadáveres e prédios destruídos. (DW, 2022)

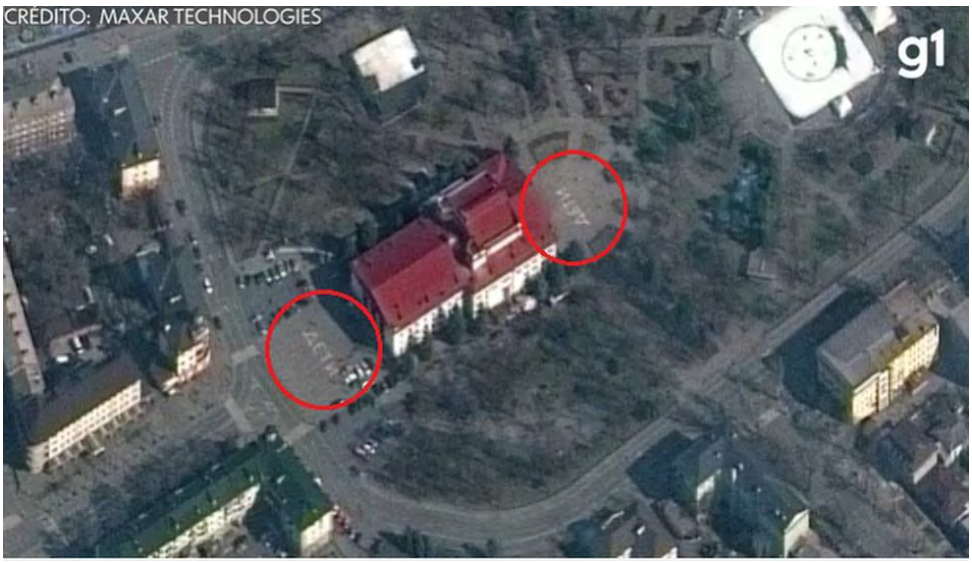

Figura 13 – Teatro de Mariupol, mostrando a palavra Criança ao chão.
Fonte: G1, 2022.

Figura 14 – Teatro de Mariupol após ataque aéreo.
Fonte: G1, 2022.

Visto que também se pode perceber o míssil atingindo o prédio residencial em Kiev, entrou no apartamento, destruindo o imóvel, lançado de maneira isolada no prédio de 15 andares, apenas em um local específico, como se o alvo estivesse naquele local. (G1, 2022) O *"Ministério da Defesa da Rússia disse que lançou ataques com mísseis de cruzeiro durante a noite contra alvos na Ucrânia – mas afirmou que visava exclusivamente a infraestrutura militar." (LISTER, 2022).* Segundo Anton Herashchenko, assessor do Ministério do Interior, aproximadamente 40 lugares como esse foram atingidos. (G1, 2022)

Figura 03 – Prédio residencial em Kiev após ser atingido por um míssil, foto divulgada no Facebook pelo prefeito de Kiev.
Fonte: CNN Brasil, 2022.

Em contrapartida das ações durante a invasão da Rússia o Google tomou medidas para fazer com que diminua o risco das pessoas se tornarem alvos e também serem afetadas pelos bombardeios. Então a Google começou a utilizar um sistema para Android trabalhando com Google Play Services, desenvolvendo-se de maneira nativa no aparelho, o usuário não precisará baixar nenhum aplicativo, sendo utilizado de maneira complementar com o governo ucraniano, para avisar os usuários dos locais que possam sofrer ataques aéreos. Além disso, o Google desativou recursos do Google Maps, para que não possa ser utilizados pelo serviço de inteligência russa, como também a suspensão do editor de serviços de mapa na região, depois de ser denunciada a ferramenta por estar sendo utilizada para coordenar ataques aéreos, onde marcava locais estratégicos na região. (GONÇALVES, 2022)

Ao compreender as derivações de espionagem adjuntas aos ataques de misseis disparados em locais civis na Ucrânia. Entende-se que o conflito de informação acontece devido ao objetivo da automatização da sociedade, que é decidir quem é confiável e quem não é. Os aliados de suas sistemáticas devem se comportar como as ideias do controle do qual se aplica, enquanto os não confiáveis são hostis pressionados e possuem rigorosos sentidos de vigilância, pois é o inimigo. Os dados agem sem levar em conta o fator de honestidade ou moralidade, é simplesmente a ordem agindo para redefinir a sociedade e colocar a sua conduta dentro da arquitetura do controle. É a mais pura ação vigilante agindo sob as aparências das informações, monitorando o sentido estético dos dados para compor suas respostas de proibição acerca das condutas do ser humano. (SADIN, 2020, p. 219-226)

Com isso se pode perceber o quanto a sociedade acaba se tornando inimiga de si mesma com a utilização da tecnologia em suma exposição da privacidade, pois da mesma acaba servindo como ferramenta para espionagem por serviço de inteligência para demarcação de alvos, e assim poder compreender os inimigos de dentro para fora. Isolando os dados, onde acaba se tornando uma ferramenta algorítmica, é parte do comportamento inteligente, é o alvo móvel. O que se coloca aqui é uma análise acerca da espionagem agindo antes e possivelmente a posteriori de um ataque, tratando o ser humano como um

polo informativo, onde os comportamentos digitais respondem as medidas hostis ou não, se o sujeito é alvo ou não.

3. RESULTADO

Com a análise desenvolvida, se pode perceber uma conduta de espionagem agindo a priori da condição humana, prevalecendo o comportamento algoritmo, onde o sujeito é parte numérica da sociedade. O que resulta a encontrar de maneira tácita a problemática no que tange a privacidade, liberdade, idealismo cibernético dominado totalmente na maneira de ser. Onde a sociedade acredita não ter algo a esconder, mas sem perceber pode vir a se tornar um alvo móvel através de seu comportamento sintetizado com base na lógica computacional e não pelo fator humano.

4. CONSIDERAÇÕES FINAIS

Se percebe acerca da estrutura espiã, que a espionagem digital é binária para se pensar numericamente o comportamento do ser humano, mediante as formações comportamentais do ser humano em rede, pois em um composto de ciberguerra, os dados são roubados, vazados e sobram apenas sombras digitais, registros de uma vida digital que se torna prova para que seja alvo, sem averiguar o fator humano. O alvo é numérico, é lógico, estruturalizado para um ataque, pois quanto mais se manifesta, mais surge e aparece em rede, maiores as chances de tornar-se inimigo de si mesmo. Onde a lógica ativa nas redes faz voltar para si em forma de alvo em consonância à vigilância virtual que comporta fomentos de hostilidade nas ações construtivas da sociedade.

O panóptico digital se manifesta em forma aguda com uma violência cega, onde misseis são lançados em prol de informações não formalizadas. Se poderia indicar: falhas referentes aos serviços de inteligência, sociedade integrada ao mundo digital, precipitação informacional em momentos de tensão, onde a única

vítima da estrutura algoritificada é o ser humano, enquanto o dado é binário, as leituras de dados são binárias.

Isso transforma a sociedade com condutas binárias entre: sim e não, positivo e negativo, certo e errado, viver ou morrer. Não há um caminho do meio do qual possa permitir compreender a linha tênue do sentido humanitário, se pula diretamente a linha para uma escolha direta sem pensar no outro.

É o composto numérico quantificado da sociedade que entra em jogo de espionagem perante a uma ciberguerra, para que as informações possam chegar as conclusões precipitadas e errôneas, colocando as vidas em risco por simplesmente escolherem determinados tipos de anúncios, registros médicos, escrevem determinadas posições pessoais em uma rede privada, assistirem o que mais lhe entretém, assuntos conversados próximos dos aparelhos celulares, produtos comprados, cliques, mapas térmicos dos dedos e mouses em um caminho de escolha, locais onde as câmeras dos celulares são espionadas sem consentimento e as pessoas são vistas sem perceberem, aparelhos celulares deixando protocolos de localização em tempo real. Tudo para aglomerar informação do alvo móvel que tem o corpo como mira de um simbolismo de observações analíticas e puramente lógicas de suas vontades e sensações. Onde o aqui e agora real, é parte da consequência de planejamentos com análises projetáveis de pré-cognições virtuais. A vida é digital, o comportamento é virtual, as ideologias são virtuais, as sensações são virtuais, mas os mísseis são reais, a morte é real.

REFERÊNCIAS

ALÓS, Javier. **Crítica de la razón precária: la vida intelectual ante la obligación de lo extraordinário**. Madrid: Catarata, 2019.

BAPNA, Sanjay; CHEN, Yan; HUA, Jian. **Industrial cyber espionage**. Journal of Management Systems, Vol. 25, 2015.

BENNETT, Richard. **The Cyberwar in Ukraine**. High Tech Forum, 2022. Disponível em: <https://hightechforum.org/the-cyberwar-in-ukraine/>. Acesso em 23 de março de 2022.

BERARDI, Franco. **Depois do futuro**. São Paulo: Ubu Editora, 2019.

DAVIES, Pascale. **Cyber espionage is key to Russia's invasion of Ukraine. The international community is fighting back**. Euronews, 2022. Disponível em: <https://www.euronews.com/next/2022/03/09/cyberespionage-is-key-to-russia-s-invasion-of-ukraine-the-international-community-is-fight>. Acesso em: 23 de março de 2022.

GALANTE, Alexandre. **Moderno avião espião russo Tu-214R é visto sobre a Síria**. Poder Aéreo, 2016. Disponível em: <https://www.aereo.jor.br/2016/08/17/moderno-aviao-espiao-russo-tu-214r-e-visto-sobre-a-siria/>. Acesso em 23 de março de 2022.

GONÇALVES, André. **Google alerta usuários do Android na Ucrânia sobre ataques aéreos**. Tecmundo, 2022. Disponível em: <https://www.tecmundo.com.br/mercado/235290-google-alerta-usuarios-android-ucrania-ataques-aereos.htm>. Acesso em 23 de março de 2022.

___. **Rússia possui 'esferas robóticas' para espionar zonas de guerra**. Tecmundo, 2022. Disponível em: <https://www.tecmundo.com.br/internet/234879-russia-possui-esferas-roboticas-espionar-zonas-guerra.htm>. Acesso em: 23 de março de 2022.

CYBERWAR: BIG TECH TAKES ON RUSSIA AS INVASION OF UKRAINE INTENSIFIES, Wral Tech Wire, 2022. Disponível em: <https://wraltechwire.com/tag/hackers/>. Acesso em: 23 de março de 2022.

HABERMAS, Jürguen. **Mudança estrutural da esfera pública**. Rio de Janeiro: Tempo Brasileiro, 2013.

HAN, Byung-Chul. **Psicopolítica: neoliberalismo y nuevas técnicas de poder**. Barcelona: Editora Herder, 2014.

HUMPHRIES, John. **O espião de Hitler**. São Paulo: Universo dos Livros, 2015.

HARDING, Luke. **Arquivos Snowden: a história secreta do homem mais procurado do mundo**. São Paulo: Texto Editores, 2014.

IT ARMY OF UKRAINE. Telegram, 2022. Disponível em: <https://t.me/s/itarmyofukraine2022>. Acesso em 25 de março de 2022.

CIBERAMEAÇA EM TEMPO REAL, Kaspersky, 2022. Disponível em: <https://cybermap.kaspersky.com/pt/stats#country=213&type=OAS&period=m>. Acesso em: 1 de agosto de 2022.

LERMAN, Rachel; ZAKRZEWSKI, Cat. **Elon Musk's Starlink is keeping Ukrainians online when traditional Internet fails**. The Washington Post, 2022. Disponível em: <https://www.washingtonpost.com/technology/2022/03/19/elon-musk-ukraine-starlink/>. Acesso em: 23 de março de 2022.

LISTER, Tim. **Prédio residencial em Kiev é atingido por míssil, diz prefeito**. CNN Brasil, 2022. Disponível em: <https://www.cnnbrasil.com.br/internacional/predio-residencial-em-kiev-e-atingido-por-missil-diz-prefeito/>. Acesso em 23 de março de 2022.

LOCHERY, Neill. **Lisboa: 1939-1945, guerra nas sombras**. Rio de Janeiro: Editora Rocco, 2011.

MARIN, Jorge. **Internet da Ucrânia tem quedas por ataques cibernéticos russos**. Tecmundo, 2022. Disponível em:

<https://www.tecmundo.com.br/internet/235316-internet-ucrania-tem-quedas-ataques-ciberneticos-russos.htm>. Acesso em: 23 de março de 2022.

MILLER, Maggie. **The world holds its breath for Putin's cyberwar**. Politico, 2022. Disponível em: <https://www.politico.com/news/2022/03/23/russia-ukraine-cyberwar-putin-00019440>. Acesso em: 25 de março de 2022.

MUNHOZ, Maurício**. Rota de fuga: a história não contada da SS**. Lisboa: Chiado Editora, 2015.

O QUE SE SABE SOBRE O ATAQUE A TEATRO EM MARIUPOL QUE PODE TER MATADO 300 PESSOAS, G1, 2022. Disponível em: <https://g1.globo.com/mundo/ucrania-russia/noticia/2022/03/25/o-que-se-sabe-sobre-o-ataque-a-teatro-em-mariupol-que-pode-ter-matado-300-pessoas.ghtml>. Acesso em: 25 de março de 2022.

PURNELL, Sonia. **Uma mulher sem importância: a história secreta da espiã americana mais perigosa da Segunda Guerra Mundial**. São Paulo: Editora Planeta, 2021.

RUIZ, Felipe. **Cyberwar from conflict in Ukraine? The emergence of WhisperGate as the first worrying sign**. Fluid Attacks - Blog, 2022. Disponível em: <https://fluidattacks.com/blog/cyberwar-ukraine/>. Acesso em: 28 de março de 2022.

SADIN, Eric. **La inteligencia artificial o el desafío del siglo: Anatomía de um anti-humanismo radical**. Buenos Aires: Caja Negra, 2020.

___. **La vie algorithmique: critique de la raison numérique**. Paris: Éditions L'échappée, 2015.

SETZER, Valdemar. **Dado, informação, conhecimento e competência**. DataGramaZero – Revista de Ciência da Informação, 1999. Disponível em: <https://www.ime.usp.br/~vwsetzer/datagrama.html>. Acesso em: 20 de março de 2022.

SHEAD, Sam. **‘We want them to go to the Stone Age’: Ukrainian coders are splitting warfare**. CNBC, 2022. Disponível em: < https://www.cnbc.com/2022/03/23/ukrainian-coders-splitting-their-time-between-day-job-and-cyberwar.html>. Acesso em: 25 de março de 2022.

SNOWDEN, Edward. **Eterna vigilância**. São Paulo: Editora Planeta, 2019.

SNOWDEN - Herói ou Traidor. Direção de Oliver Stone, Roteiro escrito por Oliver Stone e Kieran Fitzgerald. Califórnia: Endgames Entertaiment, 2016. (129 minutos).

UCRÂNIA ESTIMA QUE 300 PESSOAS MORRERAM EM ATAQUE A TEATRO. DW, 2022. Disponível em: <https://www.dw.com/pt-br/ucr%C3%A2nia-estima-que-300-pessoas-morreram-em-ataque-a-teatro/a-61261605>. Acesso em 25 de março de 2022.

VÍDEO: MÍSSIL ATINGE PRÉDIO RESIDENCIAL EM KIEV. G1, 2022. Disponível em: <https://g1.globo.com/mundo/ucrania-russia/noticia/2022/02/26/video-missil-atinge-predio-residencial-em-kiev.ghtml>. Acesso em: 23 de março de 2022.

WISNIEWSKI. Chester. **Russian-Ukraine war: related cyberattacks developments**. Sophos News, 2022. Disponível em: <https://news.sophos.com/en-us/2022/03/21/russia-ukraine-war-related-cyberattack-developments/>. Acesso em: 23 de março de 2022.

ZIZEK, Slavoj. **Bem-vindo ao deserto do real!**. São Paulo: Boitempo editorial, 2011.