Marco zero
As origens da guerra cibernética orquestrada pelos Estados Unidos para atingir a República Islâmica do Irã (2007-2010)[1]

Fernando H. Casalunga | *Eduardo Munhoz Svartman* | *Bruno Cardoso Reis*

INTRODUÇÃO

Ao passo em que cada vez mais casos envolvendo o uso do poder cibernético em conflitos interestatais, seja para realizar campanhas de reconhecimento e informação, otimizar ou comprometer sistemas operacionais militares e/ou civis de infraestruturas físicas, e/ou impactar de modo significativo a moral doméstica dos alvos atingidos vêm à tona, cresce a demanda por estudos capazes de compreender a origem do interesse dos Estados pelo desenvolvimento de capacidades táticas e operacionais neste domínio[2].

Ante ao desafio, é ponto pacífico que o problema da segurança cibernética está a exercer função ambivalente sobre as decisões estratégicas dos Estados, pois, se por um lado é preciso mitigar os riscos à segurança do funcionamento das infraestruturas críticas, por outro é necessário reconhecer que este novo domínio tem se destacado como um novo engenho de força capaz de ampliar as possibilidades de projetar poder em conflitos interestatais[3].

Frente ao cenário, as instituições securitárias norte-americanas apontam para o ciberespaço[4] como um domínio estratégico que requer o desenvolvimento de capacidades não apenas para assegurar o funcionamento adequado dos sistemas de informação responsáveis por controlar setores de infraestrutura crítica, mas, sobretudo, oferecer

RESUMO

Neste artigo realizamos um estudo de caso-único do conflito desencadeado entre os Estados Unidos e a República Islâmica do Irã (2007-2010), sob a perspectiva dos retornos estratégicos auferidos em função do uso da tecnologia da informação para atingir setores de infraestrutura crítica. Nossa análise destaca as condições que permitiram aos norte-americanos ampliarem as capacidades de projeção de poder sobre o seu adversário, fatores significativos para explicar a origem e o impacto da guerra cibernética nos dias atuais. A partir da coleta de evidências que revelam o funcionamento do mecanismo das operações orquestradas por atores estatais e não estatais para conter o programa nuclear iraniano, verificamos como o ciberespaço se tornou um domínio chave para a consecução de objetivos estratégicos nacionais. Por este prisma, com base em fontes primárias e secundárias utilizamos técnicas de análise qualitativa para responder à seguinte questão: como os Estados Unidos utilizaram o ciberespaço para atingir o programa nuclear iraniano?

Palavras-chave: guerra cibernética, poder nacional, tecnologia da informação, código malicioso.

→

 https://doi.org/10.23906/ri2024.82a06

ABSTRACT

Ground zero: the origins of the United States's cyber war against the Islamic Republic of Iran (2007-2010)

In this article, we conduct a single-case study of the conflict between the United States and the Islamic Republic of Iran (2007–10), from the perspective of the strategic returns obtained through the use of information technology to achieve criticism of infrastructure sectors. Our analysis highlights the conditions that allowed the North Americans to expand their power projection capabilities over their adversary, significant factors in explaining the origin and impact of cyber warfare today. By collecting evidence that reveals the functioning of the operational mechanism orchestrated by state and non-state actors to contain the Iranian nuclear program, we verify how cyberspace has become a key domain for achieving national strategic objectives. From this perspective, based on primary and secondary sources, we use qualitative analysis techniques to answer the following question: how did the United States use cyberspace to target the Iranian nuclear program?

Keywords: cyber warfare, national power, information technology, malicious code.

alternativas efetivas ao uso da força que não ultrapassem os limites tradicionais da guerra[5].

Diretamente conectada ao nível do poder nacional, a operação Jogos Olímpicos (2007-2010), atribuída aos Estados Unidos e Israel, afetou o programa nuclear iraniano minando as capacidades físicas e psicológicas do alvo por intermédio de campanhas de reconhecimento e exploração que resultaram no primeiro ataque cibernético cinético documentado[6].

Nesta pesquisa destacamos as condições que proporcionaram a constituição desta operação com intuito de oferecer resposta ao seguinte questionamento: como os Estados Unidos utilizaram o ciberespaço para atingir o programa nuclear iraniano? À vista disso, nosso desenho de pesquisa segue uma abordagem qualitativa para examinar o processo de uso do ciberespaço para projeção de poder nacional com base em evidências que revelam o mecanismo de ação interagências que se encontra no bojo da guerra cibernética[7].

A partir do exame de relatórios técnicos, artigos de jornal e documentos oficiais, nossa análise destaca dois fatores que permitiram aos Estados Unidos ampliarem a magnitude da assimetria de poder ante um adversário regional. Para tanto, o artigo está dividido em três seções, as quais examinam: *i*) o contexto histórico que envolve a relação entre estes adversários; *ii*) a complexidade da operação Jogos Olímpicos; *iii*) a mudança institucional na estrutura de força norte-americana.

Nossa contribuição para o campo de estudos de política internacional e defesa é marcada por ilustrar como o problema da segurança cibernética se tornou fulcral para as disputas interestatais contemporâneas. Ademais, aspiramos lançar luz sob o obscuro funcionamento do mecanismo que regula o uso do ciberespaço para consecução de objetivos estratégicos nacionais.

CONTEXTO HISTÓRICO

Com intuito de compreender as razões que colocaram os interesses norte-americanos e iranianos em rota de colisão é preciso considerar, ainda que de modo sucinto, as nuances que constituem a historicidade das relações exteriores entre estes países. Território com recursos energéticos naturais em abundância, a atual República Islâmica

do Irã esteve por mais de cinco décadas sob controle da dinastia Pahlavi, e foi durante o governo de Reza Xá Pahlavi (1925-1941) que, em 1935, o antigo reino da Pérsia foi reconhecido internacionalmente como Irã[8].

A monarquia constitucional perdurou até 1953, data em que Mohammad Reza Pahlavi, com o apoio de instituições de inteligência dos Estados Unidos, comandou um golpe de Estado que depôs Mohamed Mossadegh. Com isso, um regime autocrata foi estabelecido, dando início, dentre outras medidas, ao programa nuclear vinculado ao projeto norte-americano «Átomos para a Paz»[9] que visava alavancar o desenvolvimento internacional de tecnologia nuclear para fins de produção energética[10].

Ao longo dos anos 1960, na medida em que os norte-americanos ampliavam sua influência internacional, as relações entre estes dois Estados se fortaleciam e, em 1968, o Irã se torna signatário do Tratado de Não Proliferação de Armas Nucleares reforçando o interesse político em estreitar laços com as nações ocidentais[11]. Contudo, o processo de convulsão social que culminou na derrocada do antigo regime abalou este equilíbrio. Longe do escopo desta pesquisa examinar os meandros da Revolução Iraniana (1977--1979), cabe ressaltar que, em janeiro de 1979, estudantes islâmicos que haviam invadido a Embaixada dos Estados Unidos, em Teerã, provocaram forte tensão nas relações externas com os norte-americanos, 52 pessoas foram mantidas reféns durante a ocupação que perdurou por mais de um ano[12].

A fim de arrefecer as tensões, o conselho regente e o então primeiro-ministro Shapour Bakhtiar decidem convidar o mentor intelectual do movimento, Ruhollah Khomeini, a regressar do exílio imposto em 1964. O retorno do aiatolá e a posterior proclamação da República Islâmica do Irã, em 1979, da qual se tornou o Líder Supremo, culminou numa série de reformas que incidiram sobre as instituições civis e militares iranianas, dentre as quais, o abandono do programa nuclear[13].

A Administração Khomeini foi marcada por forte instabilidade política no Oriente Médio, a guerra travada com o Iraque (1980-1988) teve forte impacto sobre as capacidades militares iranianas ao longo do conflito. Com a morte de Khomeini um ano após o término oficial da guerra, Ali Khamenei assume o poder central. Dentre outras medidas, o novo Líder Supremo inicia o Plano AMAD (1989-2003), um conjunto de projetos para desenvolvimento e produção de tecnologia nuclear com finalidade civil e militar denominado[14].

A Administração Khamenei promove uma política externa independente que procura se aproximar com a Federação Russa no intuito de recompor o poderio bélico desgastado durante a guerra, na prática, selando o distanciamento entre o Irã e as nações ocidentais. Com a virada do século, as relações russo-iranianas se estreitaram e, em 2001, o Presidente russo Vladimir Putin tornou pública sua intenção em comercializar armas e tecnologia energética nuclear para fins pacíficos com o Irã[15].

Deste ponto em diante, as críticas da comunidade ocidental ao programa nuclear iraniano se asseveraram. Em setembro de 2002, o discurso proferido pelo Presidente

norte-americano George W. Bush classificou o Irã como um adversário pertencente ao chamado «Eixo do Mal», ao lado de Iraque e da Coreia do Norte, considerando o Estado uma ameaça à segurança internacional[16].

Neste ínterim, o sigilo em torno da construção de complexos nucleares no Irã aumentou a preocupação das agências de controle internacional que passaram a exercer pressão para monitorar suas atividades. Os iranianos permitiram que a Agência Internacional de Energia Atômica inspecionasse as instalações em 2003, por conseguinte, os relatórios publicados registraram evidências de que os processos realizados nas instalações violavam as normativas do Tratado de Não Proliferação de Armas Nucleares, em efeito, o programa nuclear foi paralisado novamente[17].

AO DELIMITAR O DESENVOLVIMENTO DE ENERGIA NUCLEAR COMO PRIORIDADE ESTRATÉGICA, A ADMINISTRAÇÃO AHMADINEJAD (2005-2013) CRIOU UM IMPASSE COM OS ESTADOS UNIDOS QUE TORNOU IRREPARÁVEL A EQUALIZAÇÃO DOS INTERESSES DE AMBOS NO ORIENTE MÉDIO.

Todavia, dois anos depois, após vencer as eleições presidenciais, Mahmmoud Ahmadinejad reativa o programa e firma um novo acordo para conclusão do complexo de Bushehr com a Federação Russa. Ao delimitar o desenvolvimento de energia nuclear como prioridade estratégica, a Administração Ahmadinejad (2005-2013) criou um impasse com os Estados Unidos que tornou irreparável a equalização dos interesses de ambos no Oriente Médio.

Destarte, a Agência Internacional de Energia Atômica e a comunidade de inteligência norte-americana apresentaram relatórios contendo evidências de que o Irã estaria empenhado em produzir artefatos bélicos nucleares[18]. Frente ao cenário, em 2006, a tensão aumentou e o Estado de Israel se uniu aos Estados Unidos nas críticas aos iranianos[19]. À altura o recurso à força tradicional foi descartado e, num esforço conjunto entre os Estados Unidos, a Organização das Nações Unidas (ONU) e a União Europeia (UE), sanções diplomáticas e econômicas foram aplicadas ao Irã. As resoluções adotadas pelo Conselho de Segurança das Nações Unidas exigiam a suspensão do programa de enriquecimento de urânio, o cumprimento dos protocolos internacionais e a constituição de controles financeiros e de exportação de materiais[20].

Conquanto, tais ações não produziram os efeitos esperados e a classe política norte-americana passou a considerar o uso de medidas alternativas para lidar com a ameaça iraniana. Em efeito, conforme veremos na seção seguinte, uma forma inédita de demonstração do poder nacional veio à tona.

GUERRA CIBERNÉTICA: A OPERAÇÃO JOGOS OLÍMPICOS (2007-2010)

Nesta seção, a fim de compreender de forma substantiva os efeitos da guerra cibernética, examinamos o ataque que atingiu setores de infraestrutura crítica do complexo nuclear de Natanz (2009-2010) no Irã em seu contexto mais amplo, na qualidade de uma operação especial que se constituiu numa cadeia de eventos interconectados que

aproximaram campanhas de reconhecimento e exploração de sistemas de informação e uso da força militar[21], considerada condição suficiente para o uso efetivo do ciberespaço para projeção de poder nacional.

De acordo com o projeto inicial, o complexo nuclear de Natanz deveria abrigar cerca de 50 mil centrífugas de enriquecimento de urânio, porém, até 2010, menos de 20% haviam sido instaladas[22], estimativas apontaram que entre 2008 e 2009 cerca de nove mil estavam operantes em Natanz[23].

Sem embargo, um acontecimento chamou a atenção da comunidade de segurança internacional quando ao menos mil delas foram substituídas sem quaisquer motivos oficialmente reportados[24]. A resposta ao enigma seria dada nos anos seguintes, através de relatórios que apresentaram evidências de que um ataque cibernético orquestrado por adversários do Irã interessados em frustrar o andamento do programa nuclear havia atingido o complexo[25].

Conforme as informações que vieram à tona a preocupação com a vulnerabilidade de sistemas de controle que operam processos críticos em infraestruturas industriais passou ao centro da agenda de instituições securitárias ao redor do mundo que buscavam compreender a configuração dos ataques, as armas utilizadas e seus efeitos[26].

Descoberto em junho de 2010, o código malicioso, posteriormente denominado «Stuxnet», fora projetado para intervir na capacidade de monitoramento e controle de processos industriais de sistemas complexos, causando falhas sequenciais que provocaram o colapso de estruturas físicas[27]. Sua identificação constitui o primeiro registro de uma arma cibernética capaz de produzir danos cinéticos.

Análises apontaram que os criadores do código possuíam conhecimento avançado sobre os parâmetros de funcionamento de sistemas ciberfísicos[28], outrossim, indicaram que a atuação conjunta entre os invasores e agências de espionagem proporcionou o acesso a informações sigilosas sobre a divisão e operação das centrífugas de Natanz. Com intuito de danificá-las, os controladores lógicos programáveis (PLC) da Siemens Simatic S7-300 (CPU 315)[29] foram estabelecidos como os principais alvos, para acessá-los, os atacantes exploraram uma ampla gama de vulnerabilidades desconhecidas de «dia-zero»[30] e invadiram os sistemas de *software* Windows da Microsoft e de supervisão e aquisição de dados (SCADA) da Siemens (SIMATIC WinCC/Step7)[31] instalados em computadores dos operadores do complexo[32].

Uma vez dentro do alvo, de forma discreta, o código malicioso executava por alguns dias uma série de rotinas de reconhecimento para mimetizar o funcionamento adequado dos rotores, em sequência, alterava periodicamente a frequência dos motores elétricos que acionavam as centrífugas e, concomitantemente, enviava informações de verificação de rotina aos operadores indicando que o processo estava sendo realizado de modo correto[33].

Ao final de 2009 o código malicioso havia afetado o módulo A26, causando falhas sequenciais em 11 cascatas interconectadas, a invasão comprometeu o funcionamento da CPU da Siemens que enviava informações aos PLC. Utilizando credenciais de acesso

remoto subtraídos das empresas RealTek e JMicron, ambas localizadas em Taiwan, os invasores foram capazes de alterar o funcionamento das centrífugas levando ao colapso ao menos mil delas, sem que os operadores tivessem conhecimento de que estavam sob ataque[34].

A análise do código malicioso chamou a atenção dos especialistas em tecnologia da informação devido à quantidade de vulnerabilidades desconhecidas utilizadas para alterar a funcionalidade dos PLC de modo imperceptível aos sensores de vigilância, ao longo das investigações quatro delas foram identificadas. Igualmente, a precisão do artefato surpreendeu, uma vez que a sabotagem ocorria apenas quando um PLC específico, conectado a um determinado tipo de dispositivo, e operando dentro de parâmetros pré-estabelecidos era identificado[35].

Cientes da ausência de conexão com redes externas nas instalações da usina, os construtores da arma cibernética a equiparam com uma vasta quantidade de informação para que pudesse atingir o alvo sem que fosse necessário qualquer comando externo para executá-lo[36]. Todavia, a engenharia por detrás de sua construção não foi o único tópico que chamou a atenção.

Análises posteriores verificaram que sua produção envolveu cerca de dez mil horas de trabalho, considerando a participação de especialistas com conhecimento avançado em interfaces operacionais da Microsoft, bem como de linguagem de gerenciamento de sistemas industriais complexos[37]. Desde a fase de experimentos até sua execução, o processo envolveu o esforço conjunto de mais de 30 programadores, a um custo de cerca de três milhões de dólares, recursos humanos e técnicos que auxiliaram na aquisição de informações sobre o funcionamento interno do complexo de Natanz, e implantação da arma nos computadores de operadores do complexo[38].

Após a ampla divulgação do Stuxnet, novas amostras derivadas de seu código fonte foram registradas revelando a complexidade desta operação, dentre as mais significativas estão os códigos maliciosos Duqu[39] e Flame[40] capazes de agir furtivamente sem que sua presença pudesse ser detectada.

As avaliações identificaram que a estrutura e os mecanismos internos de infecção do Duqu eram similares as do Stuxnet, utilizando certificados legítimos de acesso remoto de empresas privadas para enviar informações e receber comandos remotos dos invasores durante o período de exploração dos sistemas infectados. Já o Flame se propagava localmente explorando vulnerabilidades em impressoras conectadas em redes, permitindo aos invasores que obtivessem certificados legítimos indetectáveis pelos sistemas de segurança, tal qual o código original[41].

Ambos empregavam técnicas avançadas de criptografia computadorizada e foram utilizados para fins de espionagem cibernética, coletando dados confidenciais sobre a estrutura e os métodos operacionais das instalações nucleares de Natanz, movimentos que confirmaram as suspeitas de que os invasores detinham informações sobre o funcionamento interno dos equipamentos da usina e horário de trabalho dos operadores[42].

No entanto, embora tenha atrasado o programa nuclear do Irã em quase um ano, a operação não o deteve completamente, uma vez que as centrífugas danificadas foram gradativamente substituídas e as atividades retomadas[43]. Por outro ângulo, agentes securitários norte-americanos atestam que o objetivo da operação era produzir efeitos dissuasórios demonstrando aos iranianos a permeabilidade de seus sistemas operacionais[44].

Destarte, fatores como a desconfiança quanto à presença de espiões atuando em setores críticos e a possibilidade de que outros sistemas operacionais de infraestrutura de rede estivessem comprometidos, podem ter «diminuído a capacidade do Irã de adquirir poderio bélico nuclear em até dois anos – significativamente mais do que o tempo necessário para substituir as centrífugas danificadas»[45].

Não obstante, a operação quebrou o paradigma vigente dos conflitos interestatais ao demonstrar um elevado grau de precisão no uso do poder cibernético para provocar danos cinéticos de modo discreto e eficiente, fato inédito até aquele momento[46]. Por essa lógica, se tornou axiomático que os norte-americanos inauguram uma nova fase de conflitos, a qual se estabelece mediante o uso de armas cibernéticas que possuem riscos gerenciáveis e podem produzir efeitos cinéticos sem infringir os códigos internacionais de conflito armado[47].

FRENTE À DINÂMICA, A ESPIONAGEM CIBERNÉTICA EMERGE COMO OPÇÃO VALIOSA PARA PROMOVER OS INTERESSES NACIONAIS.

Frente à dinâmica, a espionagem cibernética emerge como opção valiosa para promover os interesses nacionais, pois, ainda que possamos considerar os ataques cibernéticos disruptivos e a espionagem como atividades distintas, é inegável que o uso de vetores de intrusão similares para penetrar os alvos de modo furtivo macula a linha divisória que as separa[48].

A operação permitiu que aspectos outrora puramente teóricos do fenômeno pudessem ser observados em um caso concreto, examinado e documentado por especialistas das mais diversas áreas relacionadas à segurança cibernética, condição que contribuiu para avanços na fronteira do conhecimento do uso potencial da guerra cibernética na dinâmica dos conflitos interestatais[49]. Mais do que isso, modificou a forma como as comunidades acadêmicas e de segurança passaram a enxergar a realidade objetiva das ameaças provenientes do ciberespaço, uma vez que os mecanismos de segurança vigentes se provaram insuficientes.

Frente ao exposto, naquilo que tangencia a relevância acadêmica e securitária da operação, se faz *mister* compreender como se deu o processo de mudança institucional nas forças de segurança nacional dos Estados Unidos para promover os incentivos necessários para seu desenvolvimento e posterior execução. Com base na análise de fontes oficiais, a próxima seção destaca a incorporação do domínio cibernético à estrutura de defesa norte-americana com vistas à projeção de poder nacional.

OS EFEITOS DA OPERAÇÃO JOGOS OLÍMPICOS NAS INSTITUIÇÕES SECURITÁRIAS NORTE-AMERICANAS

Nesta seção verificamos os efeitos institucionais da operação Jogos Olímpicos com base na análise de documentos oficiais, produzidos anterior e posteriormente ao fenômeno (2003-2011). O material analisado contém evidências do processo de mudança pelo qual passaram as instituições securitárias norte-americanas ao incorporarem o ciberespaço como um novo domínio de guerra, considerada condição necessária para seu uso efetivo e discreto.

Conter o programa nuclear iraniano e, assim, evitar que o país consiga obter acesso a armas de destruição em massa (ADM) que poderiam abalar o equilíbrio estratégico securitário no Oriente Médio se converteu em objetivo estratégico declarado dos Estados Unidos na primeira década deste século[50].

Neste ensejo, em 25 de novembro de 2002, a Lei de Segurança Interna promulgada pelo então Presidente George W. Bush deu origem ao Departamento de Segurança Interna (DHS), entidade constituída por vinte e duas entidades federais. Com a finalidade de se tornar o «centro federal de excelência para segurança cibernética e servir de ponto nodal da articulação entre instituições federais, estaduais, locais e não-governamentais, incluindo o setor privado, a academia e o público»[51], dentre as suas mais diversas atribuições, se destacam a coordenação de informações interagências e o fomento à pesquisa e ao desenvolvimento científico-tecnológico.

O documento formaliza a alvorada das transformações na estrutura de defesa cibernética norte-americana, dotada de forte inclinação colaborativa, por essa lógica, orienta o DHS a promover incentivos ao fortalecimento das capacidades de contenção de ameaças cibernéticas que possam afetar o funcionamento de processos industriais. A fim de mitigá-las prevê o fomento à atuação conjunta entre instituições públicas e privadas em quatro componentes do ciberespaço: «mecanismos da Internet; DCS/SCADA; correção de vulnerabilidades de *software* e *hardware*; infraestrutura física e interdependência»[52].

No que concerne à identificação e correção de vulnerabilidades em sistemas de controle industrial, frisa que códigos maliciosos representam desafios com potencial para causar danos graves ao funcionamento das infraestruturas críticas ao explorarem aberturas desconhecidas a fim de comprometer processos que regulam o funcionamento de sistemas DCS/SCADA[53].

O documento promove a cooperação entre agências de segurança e o Departamento de Defesa para coordenar pesquisas direcionadas: a proteção de setores críticos de infraestrutura, divulgação de informações, avaliação de ameaças externas às redes e sistemas de informação nacional, e investigação de crimes cibernéticos. Dentre as estruturas institucionais públicas responsáveis, destaca o Escritório de Ciência e Tecnologia, Departamento de Estado, Central de Inteligência, Departamento de Justiça e o FBI, os centros de compartilhamento e análise de informações e de resposta a emergências de computadores/centro de coordenação[54].

Por conseguinte, a Estratégia de Segurança Nacional (ESN) de 2006 assinala que o enfrentamento de novos desafios securitários depende da mudança institucional em curso, que tem na criação do DHS e instituições de inteligência seu pilar principal. O documento enfatiza os valores democráticos em oposição à tirania de grupos extremistas, tendo a liberdade e a justiça como chaves da jornada nacional de libertação dos povos: «Todas as tiranias ameaçam o interesse mundial na expansão da liberdade, e algumas, em sua busca por ADM ou patrocínio do terrorismo, ameaçam também nossos interesses imediatos de segurança»[55].

A primeira evidência da preparação de operações cibernéticas ofensivas no bojo das forças securitárias está registrada na definição dos meios necessários para conquistar os objetivos nacionais, os norte-americanos consideram agir com base no princípio da preempção no uso da força de forma controlada em ações justificáveis do ponto de vista estratégico para conter as ameaças, e citam o Irã como exemplo de Estado nocivo que objetiva adquirir artefatos nucleares e impõe restrições às liberdades políticas e religiosas aos seus cidadãos: «Nosso objetivo é convencer os adversários de que eles não podem atingir seus objetivos com ADM e, assim, dissuadi-los de tentar usar ou mesmo adquirir essas armas»[56].

OS NORTE-AMERICANOS CONSIDERAM AGIR COM BASE NO PRINCÍPIO DA PREEMPÇÃO NO USO DA FORÇA DE FORMA CONTROLADA EM AÇÕES JUSTIFICÁVEIS DO PONTO DE VISTA ESTRATÉGICO PARA CONTER AS AMEAÇAS, E CITAM O IRÃ COMO EXEMPLO DE ESTADO NOCIVO.

Tanto a ENPC (2003) quanto a ESN (2006) foram produzidas durante o período de gestação da operação Jogos Olímpicos e representam, pois, mudanças significativas que promoveram os primeiros incentivos de sua constituição. Na esteira destes documentos, a Estratégia de Defesa Nacional (EDN) de 2008 e a ESN de 2010, pontuam os meios com os quais as instituições securitárias deverão perseguir as diretrizes pré-estabelecidas.

O documento sublinha a existência de Estados desonestos como desafios de primeira ordem, e aponta para o Irã como um adversário que ameaça os interesses regionais norte-americanos devido à obscuridade de seu programa nuclear. Com intuito de resolver o problema, destaca a implementação de medidas cabíveis para assegurar a efetividade das operações militares, dentre as quais destaca aquelas com alto potencial dissuasório, mantidas abaixo do limiar da guerra tradicional: «os Estados Unidos irão, se necessário, agir preventivamente no exercício de seu direito de autodefesa para prevenir ou impedir atos hostis de nossos adversários»[57].

A segunda evidência se refere ao reconhecimento da existência de conflitos irregulares em andamento para os quais não há declaração tradicional que delimite seu início. Diante disso, os militares consideram prioritária a promoção do desenvolvimento de «capacidades de inteligência para detectar, reconhecer e analisar novas formas de guerra, bem como explorar abordagens e estratégias conjuntas para combatê-las»[58].

Por este ângulo, manifestam o interesse na incorporação de civis aos esforços da defesa, o conhecimento produzido por institutos de pesquisa e indústria é descrito como um componente significativo tanto para apoiar e garantir a efetividade das operações quanto evitar sua mobilização: «Esses desenvolvimentos exigirão uma compreensão ampliada de "conjunção", que combine perfeitamente capacidades e opções civis e militares»[59]. Ademais, dentre as metas traçadas para incrementar as capacidades da defesa, considera fulcral a parceria com o DHS que promova incentivos à constituição de operações de «penetração de redes terroristas e inteligência de medição e assinatura para identificar sistemas de distribuição de ADM»[60].

Ao final da Administração Bush (2001-2008) a operação Jogos Olímpicos foi considerada um recurso significativo para projeção de poder nacional e teve continuidade durante a administração de Barack H. Obama (2009-2017)[61]. Promulgada em maio de 2010, a ESN manteve a preocupação com proliferação de artefatos nucleares: «o maior perigo para o povo americano e para a segurança global continua a vir das ADM, particularmente o perigo representado pela busca de armas nucleares por extremistas violentos e sua proliferação para outros estados»[62].

O PROGRAMA NUCLEAR DO IRÃ É APONTADO COMO UM FATOR DE RISCO NÃO APENAS AOS SEUS VIZINHOS REGIONAIS, MAS A TODA COMUNIDADE INTERNACIONAL.

Novamente, o programa nuclear do Irã é apontado como um fator de risco não apenas aos seus vizinhos regionais, mas a toda comunidade internacional. Em vista disso, os norte-americanos reivindicaram a atitude responsiva da classe dirigente iraniana a fim de assegurar o reestabelecimento da confiança mútua, conquanto, não descartaram a possibilidade do uso de recursos estratégicos dissuasórios[63].

A terceira evidência se verifica nos indicativos da aproximação entre instituições públicas e privadas, presentes tanto na EDN (2008) quanto na ESN (2010) publicadas durante a fase sigilosa da operação Jogos Olímpicos que sugerem sua existência.

No mês seguinte daquele ano quando as informações da operação vieram a público, a engenharia institucional por detrás de sua constituição passou ao foco. Em efeito, as operações de proteção contra-ataques cibernéticos se tornaram fulcrais e o ciberespaço passou a ser considerado um domínio operacional, decisão que colocou a segurança cibernética no quadro de missões primárias do Departamento de Defesa.

Em 2011, a EDN reforçou a preocupação com a segurança cibernética e a proliferação de ADM patrocinada por Estados desonestos, como fator que colocava em questão a estabilidade regional e a segurança internacional. Nesse sentido, sublinhou a possibilidade de uso da força para impedir que o Irã obtivesse artefatos nucleares, fator que «poderia desencadear uma cascata de Estados na região em busca de paridade nuclear ou aumento das capacidades convencionais»[64].

Face ao problema, as capacidades das forças securitárias para operar no domínio cibernético ganharam relevo, em virtude disso, a quarta evidência se verifica na importância

conferida às operações dissuasórias, as quais deveriam ser orquestradas em conjunto com setores estratégicos de modo a encerrar a questão. O documento tonifica os incentivos à constituição de operações conjuntas para organizar a defesa ativa com base na cooperação interagências[65].

Diante do cenário, os militares assumem um compromisso com a produção de incentivos à cooperação entre atores estatais e não estatais para constituição de uma Força Conjunta, produto dos «comandos cibernético e estratégico, agências governamentais norte-americanas, entidades não governamentais, indústria e atores internacionais para desenvolver novas normas, capacidades, organizações e habilidades cibernéticas»[66], a fim de aprimorar os mecanismos de identificação e controle de ameaças.

Novamente, o programa nuclear do Irã foi considerado um desafio a ser superado mediante atuação das instituições securitárias nacionais e promoção de incentivos ao incremento das defesas de aliados e parceiros na região, a fim de conter o ímpeto iraniano em adquirir e/ou utilizar ADM os norte-americanos enfatizam a manutenção de «uma presença adequada capaz de tranquilizar parceiros e aliados e impedir que o Irã adquira armas nucleares»[67]. Por essa lógica, frisam o impacto tático da integração entre as capacidades operacionais militares e os esforços interagências para aquisição de informações por meio de campanhas de inteligência, vigilância e reconhecimento[68].

Com base no exame das fontes oficiais supracitadas, nossa análise registra efeitos permanentes da operação Jogos Olímpicos sobre a estrutura institucional securitária norte-americana, dentre as transformações promovidas, se destacam a criação do DHS, Comando Cibernético Norte-Americano, Força Conjunta, a Equipa de Resposta a Emergências Informáticas dos Estados Unidos, bem como sua atuação em conjunto com centros acadêmicos, setores da iniciativa privada e parceiros internacionais.

Ao explorarmos os meandros institucionais que deram origem ao fenômeno da guerra cibernética, nossa análise documental identifica as diretrizes e orientações normativas que promoveram transformações nas forças de segurança e defesa nacional norte-americanas, necessárias para garantir o uso discreto e efetivo da operação Jogos Olímpicos (2007-2010). Conforme exposto, os efeitos da criação de incentivos a constituição de movimentos desta natureza indicam não somente o nível de desenvolvimento do aparato científico e tecnológico norte-americano, mas, sobretudo, sua eficiência institucional. As evidências coletadas contribuem para sustentar o argumento de que os ataques cibernéticos que atingiram as instalações nucleares de Natanz compunham uma operação especial mais ampla, pioneira no emprego de armas cibernéticas em operações ofensivas.

CONCLUSÃO

Nesta pesquisa verificamos como o processo de mudança institucional pelo qual passaram as forças securitárias norte-americanas se conecta aos momentos críticos que culminaram no ataque cibernético às centrífugas de enriquecimento de urânio do complexo nuclear de Natanz (2009-2010).

Nossa análise identificou duas condições significativas para o emprego efetivo e discreto do ciberespaço com vistas à consecução de objetivos estratégicos dos Estados Unidos. Nesse ensejo, consideramos a operação Jogos Olímpicos um marco para os estudos de segurança por revelar o obscuro envolvimento de atores estatais e não estatais em atividades cibernéticas com consequências no mundo físico.

A operação permitiu que aspectos outrora puramente teóricos da guerra cibernética pudessem ser observados em um caso concreto, examinado e documentado por especialistas das mais diversas áreas relacionadas à defesa. De tal maneira que modificou a forma como as comunidades acadêmicas e de segurança passaram a enxergar a realidade objetiva das ameaças provenientes do ciberespaço.

Não obstante, a mudança nas instituições securitárias examinada teve efeito, sobretudo, sobre os processos de tomada de decisão, devido aos incentivos aos esforços interagências e a disponibilização de novos recursos militares moralmente superiores aos convencionais em termos de precisão e controle que permitiram à classe política norte-americana optar pelo domínio cibernético em detrimento de ataques cinéticos tradicionais para consecução de objetivos estratégicos nacionais.

Por fim, ao considerarmos a dinâmica política que circunscreve o uso do ciberespaço com intuito de auferir retornos assimétricos em um conflito regional, nossa análise enfatiza a adição de uma nova dimensão ao problema da segurança internacional, fruto da expansão dos métodos de uso da força para projeção de poder nacional disponível aos Estados, fatores que não podem ser explicados com base em conceitos tradicionais sobre a guerra. À vista disso, sublinhamos a configuração de uma nova realidade, ainda pouco explorada, que demanda esforços por parte de acadêmicos e agentes institucionais interessados em decodificar os enigmas da guerra cibernética. R:I

Data de receção: 5 de janeiro de 2024 | Data de aprovação: 5 de abril de 2024

Fernando H. Casalunga Investigador integrado do Centro de Estudos Estratégicos do Exército (CEEEx). Doutor em Ciência Política pela Universidade Federal do Rio Grande do Sul (UFRGS). Membro da Associação Brasileira de Estudos de Defesa. Atualmente desenvolve estudos sobre os impactos das instituições de inteligência no planejamento estratégico do Exército brasileiro.

> Centro de Estudos Estratégicos do Exército SMU, Brasília, DF, 70655-775, Brasil | fernandocasalunga@gmail.com

Eduardo Munhoz Svartman Professor do Departamento de Ciência Política da Universidade Federal do Rio Grande do Sul (UFRGS). Atualmente realiza estudos sobre o desenvolvimento do pensamento militar brasileiro e a introdução de sistemas de mísseis no Exército brasileiro.

> Universidade Federal do Rio Grande do Sul (UFRGS), Av. Bento Gonçalves, 9090, Agronomia, Porto Alegre, RS, 91540-000, Brasil | eduardo.svartman@ufrgs.com

Bruno Cardoso Reis Professor do Departamento de História e investigador integrado do Centro de Estudos Internacionais do Instituto Universitário de Lisboa (ISCTE). Doutor em War Studies pelo King's College. Atualmente desenvolve estudos comparados das guerras da descolonização, conflitos irregulares, grande estratégia e golpes militares.
> Instituto Universitário de Lisboa (ISCTE), Av. das Forças Armadas, 1649-026 Lisboa, Portugal | bruno.cardoso.reis@iscte-iul.pt

NOTAS

1 O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001 – no âmbito do programa PROPEX/Defesa edital n.º 14/2021.

2 KUMAR, Rajesh, et al. – «APT attacks on industrial control systems: a tale of three incidents». In *International Journal of Critical Infrastructure Protection*. Vol. 37, 2022, pp. 1-11.

3 BETZ, David J.; STEVENS, Tim – *Cyberspace and the State: Towards a Strategy for Cyber-Power*. 1.ª edição. Reino Unido: IISS Routledge, 2011.

4 Definição: domínio invisível da ação humana que se dá através de atividade eletromagnética com uso de tecnologias de informação e comunicação, se trata de um ambiente onde estão conectados e são controlados os mais diversos sistemas: financeiro, energético, transporte e telecomunicações que se constituem como infraestruturas onde ocorrem processos industriais complexos que são críticos para o funcionamento das sociedades e economias modernas. BUTRIMAS, Vytautas – «National security and international policy challenges in a post Stuxnet world». In *Lithuanian Annual Strategic Review*. Vol. 12, 2014, pp. 11-31. Consultado em: 8 de maio de 2023. Disponível em: https://kam.lt/wp-content/uploads/2022/03/lithuanian-annual-strategic-review-2013-2014-vol-12.pdf.

5 JENKINS, Ryan – «Is Stuxnet physical? Does it matter?». In *Journal of Military Ethics*. Vol. 12, N.º 1, 2013, pp. 68-79; JOLLEY, Jason – «Article 2(4) and cyber warfare: how do old rules control the brave new world?». In *International Law Research*. Vol. 2, N.º 1, 2013, pp. 1-16.

6 BRENNER, Joel – «Eyes wide shut: the growing threat of cyber attacks on industrial control systems». In *Bulletin of the Atomic Scientists*. Vol. 69, N.º 5, 2013, pp. 16-20; MILEVSKI, Lukas – Stuxnet and strategy: a special operation in cyberspace?». In *National Defense University Press*. Vol. 63, N.º 4, 2011, pp. 64-69. Consultado em: 25 de junho de 2023. Disponível em: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_64-69_Milevski.pdf?ver=Jy0SW9E8UBbatlrmrw-egQ%3D%3D.

7 MAHONEY, James – «The logic of process: tracing tests in the social sciences». In *Sociological Methods & Research*. Vol. 41, N.º 4, 2012, pp. 570-597; FALLETI, Tulia – «Process tracing of extensive and intensive processes». In *New Political Economy*. Vol. 21, N.º 5, 2016, pp. 455-462. Disponível em: https://www.tandfonline.com/doi/full/10.1080/13563467.2015.1135550.

8 AZENHA, Pedro Jorge de Oliveira – «A Estratégia Nuclear Iraniana e os Desafios Colocados à Comunidade Internacional». Lisboa: Instituto de Estudos Superiores Militares, 2010. Trabalho de Investigação Individual. Consultado em: 25 de junho de 2023. Disponível em: https://comum.rcaap.pt/handle/10400.26/12674.

9 O programa lançado em 1953 durante a Administração Dwight Eisenhower, em discurso na Assembleia Geral das Nações Unidas, abriu caminho para a constituição da Agência Internacional de Energia Atômica, entidade responsável por regular a produção de energia nuclear para fins pacíficos e fomentar o desenvolvimento de pesquisas e formação de quadros qualificados. BERMÚDEZ, Àngel – «Programa nuclear do Irã: como EUA ajudaram o país a iniciar polêmico plano atômico». BBC News Brasil. 2021. Consultado em: 15 de março de 2023. Disponível em: https://www.bbc.com/portuguese/geral-59491973.

10 MORGADE, Alba – «EUA x Irã: o que originou a rivalidade de décadas entre os dois países». BBC News Brasil. 2020. Consultado em: 24 de março de 2023. Disponível em: https://www.bbc.com/portuguese/internacional-50983943.

11 BERMÚDEZ, Àngel – «Programa nuclear do Irã...».

12 MORGADE, Alba – «EUA x Irã...».

13 AZENHA, Pedro Jorge de Oliveira – «A Estratégia Nuclear Iraniana...».

14 ALBRIGHT, David; BURKHARD, Sarah – *Entering Dangerous, Uncharted Waters: Iran's 60 Percent Highly Enriched Uranium*. WA: Institute for Science and International Security. 2022. Consultado em: 12 de agosto de 2023. Disponível em: https://isis-online.org/isis-reports/detail/entering-uncharted-waters-irans-60-percent-highly-enriched-uranium.

15 AZENHA, Pedro Jorge de Oliveira – «A Estratégia Nuclear Iraniana...», p. 11.

16 BLINDER, Caio – «Discurso do "Eixo do Mal" assombra Bush». BBC News Brasil. 2006. Consultado em: 20 de março de 2023. Disponível em: https://www.bbc.com/portuguese/reporterbbc/story/2006/10/061012_caioblinderaw.

17 ALBRIGHT, David, et al. – *Preventing Iran from Obtaining Nuclear Weapons: Restricting its Future Nuclear Options*. WA: Institute for Science and International Security. 2012. Consultado em: 27 de março de 2023. Disponível em: https://isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf.

18 *Ibidem*.

19 Os Estados Unidos e Israel começaram a considerar secretamente opções militares para atrasar a nuclearização iraniana. O nó mais importante no programa de enriquecimento do Irã na época era Natanz, uma instalação remota 150 milhas ao sul de Teerã, que iniciou suas operações industriais em fevereiro de 2007. LINDSAY, Jon – «Stuxnet and the limits of cyber warfare». In *Security Studies*. Vol. 22, N.º 3, 2013, p. 20.

20 KELSEY, Davenport – «UN Security Council Resolution on Iran». Arms Control Association. 2022. Consultado em: 26 de abril de 2023. Disponível em: https://www.armscontrol.org/factsheets/Security-Council-Resolutions-on-Iran.

21 LILIENTHAL, Gary; AHMAD, Nehaluddin – «Cyber-attack as inevitable kinetic war». In *Computer Law & Security Review*. Vol. 31, N.º 3, 2015, pp. 390-400.

22 ALBRIGHT, David, et al. – *Preventing Iran from Obtaining Nuclear Weapons*....

23 DE FALCO, Marco – *Stuxnet Facts Report: A Technical and Strategic Review*. TLL, EST: NATO Cooperative Cyber Defense Center of Excellence. 2012. Con-

sultado em: 8 de junho de 2023. Disponível em: https://ccdcoe.org/library/publications/stuxnet-facts-report-a-technical-and-strategic-analysis-2/.

24 ZETTER, Kim – «How digital detectives deciphered Stuxnet: the most menacing malware in history». WIRED Security. 2011. Consultado em: 26 de junho de 2023. Disponível em: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

25 FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric – *W32.Stuxnet Dossier*. Symantec Security Response. Califórnia: Symantec Corporation World Headquarters, 2011. Atualizado em: fevereiro de 2011. Consultado em: 26 de junho de 2023. Disponível em: https://nsarchive.gwu.edu/document/21440-document-44.

26 COLLINS, Sean; MCCOMBIE, Stephen – «Stuxnet: the emergence of a new cyber weapon and its implications». In *Journal of Policing, Intelligence and Counter Terrorism*. Vol. 7, N.º 1, 2012, pp. 80-91.

27 FARWELL, James P.; ROHOZINSKI, Rafal – «The new reality of cyber war». In *Survival: Global Politics and Strategy*. Vol. 54, N.º 4, 2012, pp. 107-120.

28 Sistemas utilizados em processos que regulam o funcionamento das infraestruturas críticas compostos por três mecanismos principais: supervisão e aquisição de dados (SCADA), controle e distribuição (DCS) e controladores lógicos programáveis (PLC). Os dois primeiros utilizam os PLC programados por operadores com acesso autorizado para executar rotinas que produzem efeitos no mundo físico. NOURIAN, ARASH; MADNICK, Stuart – «A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet». In *IEEE Transactions on Dependable and Secure Computing*. Vol. 15, N.º 1, 2018, pp. 2-13. Consultado em: 15 de junho de 2023. Disponível em: https://ieeexplore.ieee.org/document/7360168.

29 Componentes do PLC: CPU, memória e portas de entrada/saída utilizadas para ler comandos externos, ativar ou desativar impulsor de energia, exibir informações, receber comandos e ser programado. DE FALCO, Marco – *Stuxnet Facts Report…*.

30 Definição: vulnerabilidades extremamente raras e de difícil exploração que ainda não são conhecidas por fabricantes de um determinado *software* ou pelos fornecedores de antivírus. ZETTER, Kim – «How digital detectives deciphered Stuxnet…».

31 Definição: *software* Siemens que permite construir o «projeto» que contém os metadados da configuração do PLC; o passo 7 é o que permite enviar os dados para a CPU do PLC, permite a inserção do código em formato STL que envia comandos funcionais ao PLC. WinCC: software Siemens que opera em computadores pessoais para carregar o programa do PLC, envia informações sobre o andamento do processo. DE FALCO, Marco – *Stuxnet Facts Report…*.

32 DENNING, Dorothy – «Stuxnet: what has changed?». In *Future Internet Journal*. Vol. 4, N.º 3, 2012, pp. 672-687. Consultado em: 8 de maio de 2023. Disponível em: https://www.mdpi.com/1999-5903/4/3/672.

33 LINDSAY, Jon – «Stuxnet and the limits of cyber warfare».

34 ALBRIGHT, David, et al. – *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*. WA: Institute for Science and International Security. 2010. Consultado em: 26 de março de 2023. Disponível em: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

35 LANGNER, Ralph – «Stuxnet: dissecting a cyberwarfare weapon». In *IEEE Security & Privacy*. Vol. 9, N.º 3, 2011, pp. 49-51.

36 FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric – *W32.Stuxnet Dossier*.

37 COLLINS, Sean; MCCOMBIE, Stephen – «Stuxnet…».

38 DE FALCO, Marco – *Stuxnet Facts Report…*, p. 21.

39 Utiliza um documento em formato Microsoft Word para infectar os computadores das vítimas, executa de modo autônomo uma chave de entrada (*keylogger*) para registrar as teclas digitadas e salvar imagens da tela utilizada pelo usuário, outros dois arquivos corrompidos permitem aos invasores controlar os processos de registro dos usuários. GOSTEV, ALEXANDER; KUZNETSOV, Igor – «Stuxnet/Duqu: the evolution of drivers». Kaspersky. 2011. Consultado em: 23 de julho de 2023. Disponível em: https://securelist.com/stuxnetduqu-the-evolution-of-drivers/36462/.

40 Possui componentes de propagação e injeção diferenciados que reúnem registro de atividades em teclado, capturas de tela, ativação de microfone e câmera para gravação de áudio e vídeo, e sistema de Bluetooth para identificar possíveis aparelhos conectados em rede e se propagar de modo furtivo. BENCSÁTH, Boldizsár, et al. – «The cousins of Stuxnet: Duqu, Flame, and Gaus». In *Future Internet*. Vol. 4, N.º 4, 2012, pp. 971-1003.

41 MORTON, Chris – «Stuxnet, Flame e Duqu – the Olympic Games». *In* HEALEY, Jason – *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Viena, VA: Cyber Conflicts Studies Association, 2013, pp. 212-231.

42 ALBRIGHT, David, et al. – *Preventing Iran from Obtaining Nuclear Weapons…*, p. 29; DE FALCO, Marco – *Stuxnet Facts Report…*, pp. 11-27.

43 ALBRIGHT, David; BURKHARD, Sarah – *Entering Dangerous, Uncharted Waters…*; LINDSAY, Jon – «Stuxnet and the limits of cyber warfare».

44 HAYDEN, Michael – *Playing to the Edge: American Intelligence in the Age of Terror*. Nova Iorque: Penguin Press, 2016.

45 KELLO, Lucas – «The meaning of the cyber revolution perils to theory and statecraft». In *International Security*. Vol. 38, N.º 2, 2013, p. 23. Consultado em: 13 de março de 2023. Disponível em: https://www.jstor.org/stable/24480929. Salvo indicação em contrário todas as citações são traduções livres dos autores.

46 BUTRIMAS, Vytautas – «National security and international policy challenges…»; DE FALCO, Marco – *Stuxnet Facts Report…*.

47 Para um aprofundamento sobre como as normas multilaterais que limitam os conflitos interestatais tornam estratégico para os Estados o recurso às armas cibernéticas ver JENKINS, Ryan – «Is Stuxnet physical? Does it matter?».

48 BRENNER, Joel – *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. 1.ª edição. Inglaterra: Penguin Press, 2011.

49 DE FALCO, Marco – *Stuxnet Facts Report…*.

50 ALBRIGHT, David; BURKHARD, Sarah – *Entering Dangerous, Uncharted Waters…*, p. 112.

51 *NATIONAL STRATEGY to Secure Cyberspace*. Washington DC: America's Cyber Defense Agency, 2003. Consultado em: 8 de agosto de 2023. Disponível em: https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.

52 *Ibidem*, pp. 29-30.

53 *Ibidem*, p. 33.

54 *Ibidem*, pp. 28-41.

55 «NATIONAL SECURITY Strategy». Washington DC: Office of the Secretary of Defense, 2006, p. 3. Consultado em: 10 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Security-Strategy/.

56 *Ibidem*, p. 18.

57 «NATIONAL DEFENSE Strategy». Washington DC: Office of the Secretary of Defense, 2008, p. 14. Consultado em: 11 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Defense-Strategy/.

58 *Ibidem*, p. 4.

59 *Ibidem*, p. 18.

60 *Ibidem*, p. 19.

61 SANGER, David – «Obama order sped up wave of cyberattacks against Iran». In *New York Times*. 2012. Consultado em: 21 de junho de 2023. Disponível em: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

62 «NATIONAL SECURITY Strategy». Washington DC: Office of the Secretary of Defense, 2010, p. 4. Consultado em: 12 de

julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Security-Strategy/.

63 *Ibidem*, pp. 23-24.

64 «NATIONAL DEFENSE Strategy». Washington DC: Office of the Secretary of Defense, 2011, p. 3. Consultado em: 15 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Military-Strategy/.

65 *Ibidem*, pp. 3-8.

66 *Ibidem*, p. 10.

67 *Ibidem*, pp. 11-12.

68 *Ibidem*, pp. 19-20.

BIBLIOGRAFIA

ALBRIGHT, David; BRANNAN, Paul; STRICKER, Andrea; WALROND, Christina; WOOD, Houston – *Preventing Iran from Obtaining Nuclear Weapons: Constraining its Future Nuclear Options*. WA: Institute for Science and International Security. 2012. Consultado em: 27 de março de 2023. Disponível em: https://isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf.

ALBRIGHT, David; BRANNAN, Paul; WALROND, Christina – *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*. WA: Institute for Science and International Security. 2010. Consultado em: 26 de março de 2023. Disponível em: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

ALBRIGHT, David; BURKHARD, Sarah – *Entering Dangerous, Uncharted Waters: Iran's 60 Percent Highly Enriched Uranium*. WA: Institute for Science and International Security. 2022. Consultado em: 12 de agosto de 2023. Disponível em: https://isis-online.org/isis-reports/detail/entering-uncharted-waters-irans-60-percent-highly-enriched-uranium.

AZENHA, Pedro Jorge de Oliveira – «A Estratégia Nuclear Iraniana e os Desafios Colocados à Comunidade Internacional». Lisboa: Instituto de Estudos Superiores Militares, 2010. Trabalho de Investigação Individual. Consultado em: 25 de junho de 2023. Disponível em: https://comum.rcaap.pt/handle/10400.26/12674.

BENCSÁTH, Boldizsár; PÉK, Gábor; BUTTYÁN, Levente; FÉLEGYHÁZI, Márk – «The cousins of Stuxnet: Duqu, Flame, and Gaus». In *Future Internet*. Vol. 4, N.º 4, 2012, pp. 971-1003. DOI:https://doi.org/10.3390/fi4040971.

BENNET, Andrew; CHECKEL, Jeffrey T., ed. lit. – *Process Tracing: From Metaphor to Analytic Tool*. 1.ª edição. Nova Iorque: Cambridge University Press, 2014.

BERMÚDEZ, Ângel – «Programa nuclear do Irã: como EUA ajudaram o país a iniciar polêmico plano atômico». BBC News Brasil. 2021. Consultado em: 15 de março de 2023. Disponível em: https://www.bbc.com/portuguese/geral-59491973.

BETZ, David J.; STEVENS, Tim – *Cyberspace and the State: Towards a Strategy for Cyber-Power*. 1.ª edição. Reino Unido: IISS Routledge, 2011.

BLINDER, Caio – «Discurso do "Eixo do Mal" assombra Bush». BBC News Brasil. 2006. Consultado em: 20 de março de 2023. Disponível em: https://www.bbc.com/portuguese/reporterbbc/story/2006/10/061012_caioblinderaw.

BRENNER, Joel – *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. 1.ª edição. Inglaterra: Penguin Press, 2011.

BRENNER, Joel – «Eyes wide shut: the growing threat of cyber attacks on industrial control systems». In *Bulletin of the Atomic Scientists*. Vol. 69, N.º 5, 2013, pp. 16-20. DOI: https://doi.org/10.1177/0096340213501372.

BUTRIMAS, Vytautas – «National security and international policy challenges in a post Stuxnet world». In *Lithuanian Annual Strategic Review*. Vol. 12, 2014, pp. 11-31. Consultado em: 8 de maio de 2023. Disponível em: https://kam.lt/wp-content/uploads/2022/03/lithuanian-annual-strategic-review-2013-2014-vol-12.pdf.

COLLINS, Sean; MCCOMBIE, Stephen – «Stuxnet: the emergence of a new cyber weapon and its implications». In *Journal of Policing, Intelligence and Counter Terrorism*. Vol. 7, N.º 1, 2012, pp. 80-91. DOI: http://dx.doi.org/10.1080/18335330.2012.653198.

DE FALCO, Marco – *Stuxnet Facts Report: A Technical and Strategic Review*. TLL, EST: NATO Cooperative Cyber Defense Center of Excellence. 2012. Consultado em: 8 de junho de 2023. Disponível em: https://ccdcoe.org/library/publications/stuxnet-facts-report-a-technical-and-strategic-analysis-2/.

DENNING, Dorothy – «Stuxnet: what has changed?». In *Future Internet Journal*. Vol. 4, N.º 3, 2012, pp. 672-687. Consultado em: 8 de maio de 2023. Disponível em: https://www.mdpi.com/1999-5903/4/3/672.

FALLETI, Tulia – «Process tracing of extensive and intensive processes». In *New Political Economy*. Vol. 21, N.º 5, 2016, pp. 455-462. DOI: https://www.tandfonline.com/doi/full/10.1080/13563467.2015.1135550.

FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric – *W32.Stuxnet Dossier*. Symantec Security Response. Califórnia: Symantec Corporation World Headquarters, 2011. Atualizado em: fevereiro de 2011. Consultado em: 26 de junho de 2023. Disponível em: https://nsarchive.gwu.edu/document/21440-document-44.

FARWELL, James P.; ROHOZINSKI, Rafal – «The new reality of cyber war». In *Survival: Global Politics and Strategy*. Vol. 54, N.º 4, 2012, pp. 107-120. DOI: http://dx.doi.org/10.1080/00396338.2012.709391.

GOSTEV, ALEXANDER; KUZNETSOV, Igor – «Stuxnet/Duqu: the evolution of drivers». Kaspersky. 2011. Consultado em: 23 de julho de 2023. Disponível em: https://securelist.com/stuxnetduqu-the-evolution-of-drivers/36462/.

HAYDEN, Michael – *Playing to the Edge: American Intelligence in the Age of Terror*. Nova Iorque: Penguin Press, 2016.

JENKINS, Ryan – «Is Stuxnet physical? Does it matter?». In *Journal of Military Ethics*. Vol. 12, N.º 1, 2013, pp. 68-79. DOI: https://doi.org/10.1080/15027570.2013.782640.

JOLLEY, Jason – «Article 2(4) and cyber warfare: how do old rules control the brave new world?». In *International Law Research*. Vol. 2, N.º 1, 2013, pp. 1-16. DOI: http://dx.doi.org/10.5539/ilr.v2n1p1.

KELLO, Lucas – «The meaning of the cyber revolution perils to theory and statecraft». In *International Security*. Vol. 38, N.º 2, 2013, pp. 7-40. Consultado em: 13 de março de 2023. Disponível em: https://www.jstor.org/stable/24480929.

KELSEY, Davenport – «UN Security Council Resolution on Iran». Arms Control Association. 2022. Consultado em: 26 de abril de 2023. Disponível em: https://www.armscontrol.org/factsheets/Security-Council-Resolutions-on-Iran.

KUMAR, Rajesh; KELA, Rohan; SINGH, Siddhant; TRUJILLO-RASUA, Rolando – «APT attacks on industrial control systems: a tale of three incidents». In *International Journal of Critical Infrastructure Protection*.

Vol. 37, 2022, pp. 1-11. DOI: https://doi.org/10.1016/j.ijcip.2022.100521.

LANGNER, Ralph – «Stuxnet: dissecting a cyberwarfare weapon». In *IEEE Security & Privacy*. Vol. 9, N.º 3, 2011, pp. 49-51. DOI: 10.1109/MSP.2011.67.

LINDSAY, Jon – «Stuxnet and the limits of cyber warfare». In *Security Studies*. Vol. 22, N.º 3, 2013, pp. 365-404. DOI: https://doi.org/10.1080/09636412.2013.816122.

LILIENTHAL, Gary; AHMAD, Nehaluddin – «Cyber-attack as inevitable kinetic war». In *Computer Law & Security Review*. Vol. 31, N.º 3, 2015, pp. 390-400. DOI: https://doi.org/10.1016/j.clsr.2015.03.002.

MAHONEY, James – «The logic of process: tracing tests in the social sciences». In *Sociological Methods & Research*. Vol. 41, N.º 4, 2012, pp. 570-597. DOI: https://doi.org/10.1177/0049124112437709.

MILEVSKI, Lukas – Stuxnet and strategy: a special operation in cyberspace?». In *National Defense University Press*. Vol. 63, N.º 4, 2011, pp. 64-69. Consultado em: 25 de junho de 2023. Disponível em: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_64-69_Milevski.pdf?ver=Jy0SW9E8UBbatlrmrw-egQ%3D%3D.

MORGADE, Alba – «EUA x Irã: o que originou a rivalidade de décadas entre os dois países». BBC News Brasil. 2020. Consultado em: 24 de março de 2023. Disponível em: https://www.bbc.com/portuguese/internacional-50983943.

MORTON, Chris – «Stuxnet, Flame e Duqu – the Olympic Games». *In* HEALEY, Jason – *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Viena, VA: Cyber Conflicts Studies Association, 2013, pp. 212-231.

«NATIONAL DEFENSE Strategy». Washington DC: Office of the Secretary of Defense, 2008. Consultado em: 11 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Defense-Strategy/.

«NATIONAL DEFENSE Strategy». Washington DC: Office of the Secretary of Defense, 2011. Consultado em: 15 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Military-Strategy/.

«NATIONAL SECURITY Strategy». Washington DC: Office of the Secretary of Defense, 2006. Consultado em: 10 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Security-Strategy/.

«NATIONAL SECURITY Strategy». Washington DC: Office of the Secretary of Defense, 2010. Consultado em: 12 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Security-Strategy/.

NATIONAL STRATEGY to Secure Cyberspace. Washington DC: America's Cyber Defense Agency, 2003. Consultado em: 8 de agosto de 2023. Disponível em: https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.

NOURIAN, ARASH; MADNICK, Stuart – «A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet». In *IEEE Transactions on Dependable and Secure Computing*. Vol. 15, N.º 1, 2018, pp. 2-13. Consultado em: 15 de junho de 2023. Disponível em: https://ieeexplore.ieee.org/document/7360168.

SANGER, David – «Obama order sped up wave of cyberattacks against Iran». In *New York Times*. 2012. Consultado em: 21 de junho de 2023. Disponível em: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

ZETTER, Kim – «How digital detectives deciphered Stuxnet: the most menacing malware in history». WIRED Security. 2011. Consultado em: 26 de junho de 2023. Disponível em: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.