O Necessário *Upgrade* na Ciberdefesa Brasileira

Marcelo Antonio Osller Malagutti - Escola de Comando e Estado Maior do Exército (ECEME)

Resumo

Este artigo tece análises e considerações sobre a necessidade de se processar um upgrade no Comando de Defesa Cibernética (ComDCiber) para o atendimento das necessidades do Brasil, considerando aspectos como o posicionamento do órgão dentro da estrutura organizacional da defesa brasileira, sua missão e estrutura, e também aspectos relativos ao dimensionamento, aquisição e retenção de membros da equipe, militares e civis.

Palavras-chave: Ciberdefesa; Cibersegurança; Ciberameaças.

Abstract

This article analyses the need of upgrading Brazilian Cyber Defence Command (ComDCiber) to meet the needs of the country, considering aspects such as the placement of the body within the organizational structure of Brazilian Ministry of Defence, its mission and structure, as well as aspects related to the sizing, acquisition and retention of personnel, either military and civilian.

Keywords: Cyber Defence; Cyber Security; Cyber Organisations.

Introdução

O avanço da cibernética foi, em grande medida, originado por pesquisas patrocinadas pelas forças armadas modernas. Em Bletchley Park, em 1941, Alan Turing e sua equipe criaram a *Bombe*, o primeiro computador da história. O equipamento, ainda eletromecânico, ajudou a decifrar o código Enigma, utilizado pelas forças armadas nazistas. Em 1943, no mesmo local, Tommy Flowers e sua equipe criaram o Colossus Mark I, o primeiro computador eletrônico, o qual permitiu a decifragem do ultrassecreto código Lorenz, usado por Hitler e pelo Alto Comando alemão. Ambas as máquinas foram ativos importantes para a vitória na Segunda Guerra Mundial (GCHQ 2016).

Também em 1943, o exército americano encomendou à Universidade da Pensilvânia o desenvolvimento de uma máquina para cômputos balísticos, resultando no ENIAC, primeiro computador eletrônico programável, operacionalizado em 1946. O medo de bombardeios em território norte-americano, como ocorridos em Londres na WWII, resultou na criação do Semi-Automatic Ground Environment (SAGE, "sábio" em inglês), integrando centenas de estações de radar com 23 supercomputadores distribuídos pelos EUA, cujo protótipo funcionou em 1951 (Rid 2016, 76–77). O sistema, contratado à IBM, utilizava linhas de comunicação comerciais da AT&T para integrar a rede, centralizada em 1958 no mítico North-American Air Defense Command (NORAD), ao custo total atualizado superior a 500 bilhões de dólares, despendidos em 15 anos (Rid 2016, 76–77). A Advanced Research Projects Agency (ARPA), do Pentágono, objetivando melhorar sistemas de comando e controle militares e prover redundância de rotas em casos de falhas de algum nó dessa rede, custeou o desenvolvimento da ARPANET, a famosa precursora da Internet (Rid 2016, 111; 147).

No Brasil o impulso inicial à informática também esteve ligado aos militares. Influenciado pelas ideias do Capitão de Corveta Geraldo Maia, recém retornado de seu mestrado nos EUA, em 1958, o Governo Juscelino Kubitscheck criou um grupo para avaliar o uso de computadores na administração pública, o qual, no ano seguinte, autorizou a importação dos três primeiros computadores do país (Moreira 1995, 23–24).

Para lidar com as ameaças postas pelo ciberespaço, o quinto domínio da guerra, estados nacionais criam comandos militares e/ou de inteligência cibernética e reforçam seus arsenais. Uma análise extensiva das ofensas cibernéticas promovidas por estados foge ao escopo deste trabalho, podendo ser encontrada alhures[1]. No presente trabalho analisa-se as estruturas de ciberdefesa[2] e cibersegurança criadas ou adaptadas por Estados Unidos, Reino Unido, China, Alemanha, França e Brasil para fazer frente às ameaças percebidas.

EUA, China e Rússia são os mais citados atores estatais no ambiente cibernético. São frequentemente responsabilizados por ataques a diversos países, comumente entre eles mesmos. Especialistas dos EUA alegam que os russos são definitivamente melhores que os chineses e que são "quase tão bons como os próprios norte-americanos", mas os chineses recebem mais atenção porque, intencionalmente ou não, têm deixado muitas vezes rastros em suas ações, sendo mais "barulhentos" nas redes (Segal 2016, 115). Contudo, outros atores também surgem como protagonistas nesta área, como é o caso da Alemanha, França, Reino Unido, Israel, Irã, Coreia do Norte e Austrália (Breene 2016; Rugge 2018; Voo et al. 2020).

Casos renomados como *Stuxnet*, *Snowden*, *Wikileaks*, *Prykarpattyaoblenergo* e *CrashOverride*[3] exemplifi-

1 Para mais detalhes ver Malagutti (2016).

2 O presente texto utiliza preferencialmente a nomenclatura em língua portuguesa adotada pela União Europeia, consoante com o novo Acordo Ortográfico da Língua Portuguesa, combinando o prefixo ciber com os substantivos aos quais se refere, como em ciberespaço, ciberameaças, ciberofensas, cibersegurança e ciberdefesa (Parlamento Europeu 2018).

3 *Stuxnet*, alegadamente, foi um malware desenvolvido pelos EUA e

cam como estados nacionais utilizam o ciberespaço como um espaço geopolítico, promovendo o poder do estado e buscando influenciar decisões de atores capazes de fazerem escolhas críticas no curso de um conflito, seja por meio da aplicação de força potencial ou real, caracterizando *coerção*, ou da obtenção de informações privilegiadas, caracterizando ações de *inteligência* (Malagutti 2017).

Como regra geral, num contexto que Beaufre (1998, 22) denominou "dialética de vontades opostas", dentro de uma racionalidade de custos, benefícios e riscos, dois estados, A e B, agirão assim: A empregará todas as expressões de poder (econômico, político, militar, científico-tecnológico ou psicossocial) disponíveis para *compelir* B a atender aos interesses de A; simultaneamente, B empregará seu poder para *dissuadir* A de tentar compelir B a curvar-se aos interesses de A (Malagutti 2017).

Este artigo apresenta considerações relativas a um Comando de Defesa Cibernética de natureza militar, incluindo seu posicionamento lógico dentro da estrutura organizacional da defesa brasileira, sua missão, estrutura, dimensionamento, aquisição e retenção de pessoal. Os aspectos aqui discutidos, a despeito de sua relevância, não exaurem o tema. O estudo se pauta em uma análise comparada de estruturas de ciberdefesa dos países acima citados, realizado com base em análise qualitativa de conteúdo (Bardin 2016). As fontes utilizadas são documentos oficiais, artigos acadêmicos, relatórios de think tanks, livros e matérias jornalísticas de profissionais e instituições renomados internacionalmente na área da ciberdefesa e cibersegurança.

Análise Comparada da Ciberdefesa em Diferentes Países

Em 2010, o Brasil parecia querer alinhar-se a seus pares em segurança cibernética. Após a publicação de Cyberwar (Clarke and Knake 2010) e na esteira das primeiras revelações do Stuxnet, o Exército Brasileiro criou o núcleo de seu Centro de Defesa Cibernética, enquanto Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (GSI), criado já em 2006, publicou o Livro Verde da Cibersegurança, no que atualmente é denominado DSIC (Mandarino and Canongia 2010).

Porém, foi apenas dez anos depois, em fevereiro de 2020, que o Brasil publicou sua primeira estratégia nacional para o ciberespaço, batizada de e-Ciber (Brasil-GSI 2020). Foi o penúltimo país a fazê-lo entre as 15 maiores economias: Estados Unidos, China, Japão, Alemanha, Índia, Reino Unido, França, Itália, Brasil, Canadá, Rússia, Coreia do Sul, Espanha, Austrália e México (IMF 2019).

Além de tardia, a e-Ciber trouxe uma *jaboticaba*[4]: trata apenas de cibersegurança, intencionalmente excluindo ciberdefesa[5]. Nenhum outro país dentre os citados nesta

Israel com o objetivo de danificar as centrífugas de refinamento de urânio da central nuclear de Natanz, retardando o programa nuclear iraniano e coagindo aquele país a aceitar a fiscalização de suas instalações por parte da Agência Nacional de Energia Atômica (Zetter 2011; Langner 2011; Falliere, Murchu, and Chien 2011; Zetter 2014). O caso *Snowden* consistiu na revelação, por parte de Edward Snowden, empregado terceirizado da National Security Agency (NSA) dos EUA, de documentos secretos revelando ações de espionagem daquele país contra diversos de seus aliados, bem como da monitoração de comunicações eletrônicas de seus próprios cidadãos (Rusbridger 2013; Sanger and Schmitt 2014; Greenwald 2014). *Wikileaks*, um sítio na Internet criado por Julian Assange, tornou públicos milhares de documentos secretos do governo dos EUA, criando protestos internacionais e constrangimento político e diplomático para aquele país (Rosenzweig 2013, 59–62; Wilentz 2014). *Prykarpattyaoblenergo* e *CrashOverride* consistiram em ataques cibernéticos a instalações de energia elétrica da ucrânia, alegadamente por hackers russos, visando desestabilizar o suporte popular à guerra separatista na Ucrânia e a demonstrar as capacidades russas de realizar ataques contra infraestruturas elétricas (o assim-chamado *grid*), temido pelas potências ocidentais (Zetter 2016; Auchard and Finkle 2016; Dragos 2017).

4 A fruta jaboticaba (ou jabuticaba) existe apenas no Brasil, e adota-se popularmente seu nome para indicar uma peculiaridade brasileira.

5 A cibersegurança (ou segurança cibernética) consiste em ações de prevenção e combate a ciberofensas patrocinadas por atores não-estatais ou cibercrime, enquanto a ciberdefesa (ou defesa cibernética) consiste em ações contra ciberofensas patrocinadas por estados. A ciberespionagem política e militar, embora patrocinada por estados, é comumente considerada cibersegurança, sendo usualmente combatida e investigada primordialmente por forças policiais, embora frequentemente com apoio dos militares.

pesquisa faz tal separação entre cibersegurança e ciberdefesa em suas estratégias nacionais. O argumento utilizado para justificar esse fracionamento na estratégia brasileira é o de que a Política Nacional de Segurança da Informação (PNSI) prevê uma Estratégia Nacional de Segurança da Informação 'será dividida nos seguintes módulos, **entre outros**':

- I – Segurança Cibernética;
- II – Defesa Cibernética;
- III – Segurança de Infraestruturas Críticas;
- IV – Segurança de Informações Sensíveis; e
- V – Proteção contra o vazamento de dados.' (Brasil-GSI 2018 Artigo 6, grifo nosso)

Curiosamente, a e-Ciber trata também da segurança cibernética de infraestruturas críticas, enfraquecendo o argumento para a exclusão da Defesa Cibernética de seu escopo. Uma análise mais detalhada dessa e de outras idiossincrasias da e-Ciber, no entanto, foge ao escopo do presente trabalho.

Ocorre que, de 2010 a 2020, os "pares" do Brasil movimentaram-se mais rapidamente, alocando recursos significativos a suas estruturas de ciberdefesa.

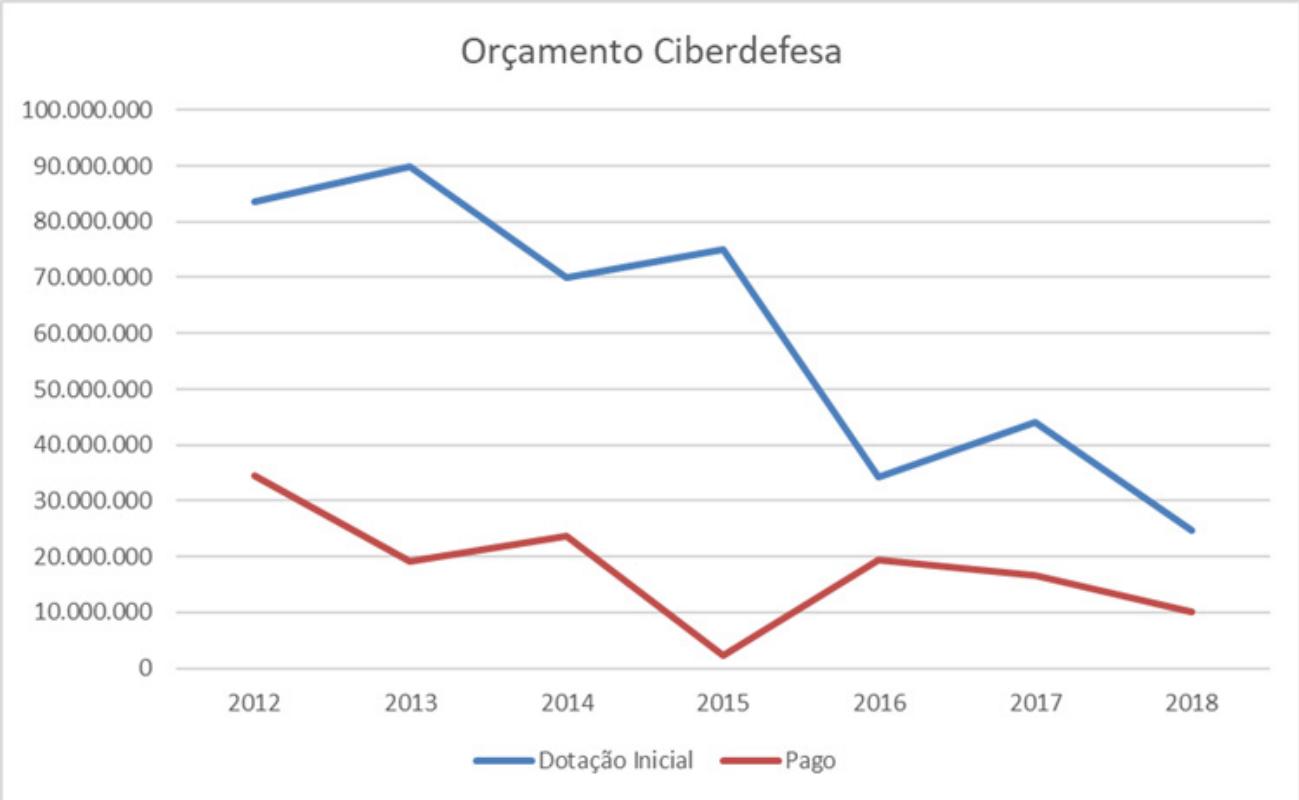
Em 2014, quatro anos após a criação do USCyberCom, os EUA anunciaram sua intenção de, até 2018, criarem uma Cyber Mission Force (CMF), a ser constituída por 133 Cyber Mission Teams (CMTs), distribuídos entre as diferentes forças singulares do país e totalizando 6.200 profissionais, operacionalmente preparados para atuação operações cibernéticas militares ofensivas e defensivas (U.S. ArmyCyber 2020). Em agosto de 2017, o USCyberCom recebeu o status de Full Combatant Command. Assim, tornou-se independente do USStratCom (Comando Estratégico), portanto com melhores condições de gerir seu próprio orçamento (Marks 2017).

O Reino Unido, por sua vez, em 2015 anunciou a recriação do 77th Battalion, com 1.500 integrantes, com a finalidade de combate à guerra informacional, com foco nas redes sociais (Paganini 2015). Em 2016, no lançamento de sua Cyber Security Strategy 2016-2021, anunciou investimentos de £ 1,9 bilhões (13,5 bilhões de Reais, em valores atuais) em 10 anos na cibersegurança daquele país (United Kingdom 2016). O valor corresponde a uma média de 1,35 bilhão de Reais anuais. Em 2017 foi anunciada a National Cyber Force, uma força de natureza eminentemente ofensiva, vinculada ao Ministry of Defence e ao GCHQ (agência de SIGINT do Reino Unido), dispondo de um efetivo inicial de 500 profissionais das Forças Armadas, GCHQ e terceirizados, que deve ser ampliado para 2.000 profissionais em três anos, ao custo de 250 milhões de Libras Esterlinas (GBP), ou 1,78 bilhões de Reais (Haynes 2018; Sabbagh 2020).

A Austrália, em agosto de 2020, publicou uma nova versão de sua Cyber Security Strategy (Australia 2020). O documento prevê investimentos do governo australiano no montante de 1,67 bilhões de dólares australianos (AUD), ou 6,5 bilhões de Reais, ao longo de 10 anos (Australia 2020, 4). Ressalta, ainda, que sua precursora, a ciberestratégia de 2016, promoveu um investimento de AUD 230 milhões (cerca de 900 milhões de Reais) em seus quatro anos de vigência (Australia 2020, 8). Outrossim, o investimento médio do governo australiano foi de 225 milhões de Reais ao ano entre 2016-2020 e deve ser de 650 milhões de Reais por ano entre 2020-2024. O investimento seria justificado com base em estimativas de que incidentes cibernéticos podem causar prejuízos de até AUD 29 bilhões, ou 1,9% do PIB do país, ao ano (Australia 2020, 10).

Já a e-Ciber brasileira não faz qualquer menção a valores de investimentos. Um relatório do Senado Federal apontou que o orçamento da ciberdefesa brasileira em 2020 é de apenas 22 milhões de Reais, dos quais apenas 6,1 milhões destinados ao ComDCiber (Amin 2019, 56). Mais que isso, conforme demonstra a Figura 1, o valor vem decrescendo ao longo dos anos, no sentido inverso ao que se observa nos demais países.

Figura 1: Evolução do Orçamento Brasileiro de Ciberdefesa



Fonte: Elaborada pelo autor a partir de dados de Amin (2019, 55)

O relatório do Senado Federal aponta, ademais, que os prejuízos decorrentes de incidentes cibernéticos em empresas brasileiras, em 2018, teriam sido de USD 20 bilhões, ou AUD 28 bilhões, montante similar ao das perdas australianas (Amin 2019, 25). Não obstante, em termos comparados, o orçamento brasileiro de cibersegurança corresponde a apenas 3% daquele australiano. A despeito do fato do PIB australiano corresponder a cerca de 70% do brasileiro. O relatório sugere que o valor deveria ser de 60 milhões para 2020, e de 120 milhões por ano nos três anos subsequentes (Amin 2019, 56).

A Tabela 1 mostra dados públicos sobre estruturas de ciberdefesa de vários países, considerando agências de inteligência e contrainteligência de sinais, cibersegurança (civil) e ciberdefesa (militar) e o ano de publicação de suas primeiras ciberestratégias.

Tabela 1 – Organizações Ligadas à Defesa e Segurança Cibernéticas. Compilada pelo autor.

País	Intel.	Contra Intel.	Seg. Civil	Defesa	Ataque	1ª Estrat. Nac. Seg. Ciber.	Efetivos
Estados Unidos	NSA CIA NGA	FBI	DHS NIST	NSA	USCyberCom	2003	7.000 (NSA) 6.200 (USCyberCom)
China	3º Dep (EM-EPL)	3º Dep (EM-EPL)	3º Dep (EM-EPL)	4º Dep (EM-EPL)	4º Dep (EM-EPL)	2003	"centenas ou milhares" (Unit 61398)
França	DGSE	DGSI	ANSSI	CALID	ComCyber	2008	3.500 (CyberCom) 600 (ANSSI)
Reino Unido	GCHQ (NCSC)	GCHQ (NCSC)	GCHQ (NCSC)	GCHQ (NCSC)	GCHQ & MoD	2009	1.900+ (NCSC) 2.000 (NCF)
Alemanha	BND BSI KSA	BfV	BSI	CIR	CIR	2011	13.600 (CIR)
Brasil	Não há	Não há	GSI/DSIC	ComDCiber	ComDCiber	2020	180~

Fontes: (Pernik, Wojtkowiak, and Verschoor-Kirss 2016; Osula 2015; Raud 2016; Schulte 2017; Brangetto 2015; Brasil-CN 2014, 137; Stokes 2015; Barlouet 2016; Hayden 2016, 127–52; Osborne 2015)

Dos países acima listados, Alemanha e China optaram pela criação de forças singulares independentes, enquanto EUA, França[6] e Reino Unido atuam com comandos que reúnem efetivos das diferentes forças singulares sob um comando unificado, subordinados ao Estado-Maior Conjunto ou a um comando estratégico nacional, embora mantendo também equipes dedicadas à defesa das redes específicas de suas forças singulares. Tais ações visam assegurar maior coesão dos esforços de ciberdefesa. À exceção do Brasil, todos integram suas forças de ciberdefesa com suas agências de inteligência de sinais (SIGINT), e em todos eles o comando da ciberdefesa militar é exercido por um oficial general de 4 estrelas, o mais elevado posto militar em condições de paz.

A Peculiar Organização da Ciberdefesa Brasileira

Dentre os países analisados, o Brasil optou por uma organização singular. A atual estrutura da ciberdefesa brasileira é composta pelo Comando de Defesa Cibernética (ComDCiber), um "comando conjunto" subordinado ao Comando do Exército (Exército Brasileiro). Ainda que se possa usar argumentos políticos para se tentar justificar essa opção, ela constitui uma *jabuticaba*[7]. *Outrossim, diferentemente dos casos do programa nuclear, a cargo exclusivo da Marinha, e do programa espacial, a cargo exclusivo da Força Aérea, a defesa cibernética, embora seja atribuição estratégica do Exército, constitui um comando conjunto das três FAs singulares. Conceitualmente, esperar-se-ia que um comando conjunto fosse vinculado ao Estado-Maior Conjunto das Forças Armadas (EMCFA) ou ao Ministro da Defesa (MD), a exemplo do que ocorre nos demais países acima analisados, e não a uma força singular. Aliás, isso é o que estipula a Lei Complementar 136, de 2010, em seu artigo 15, inciso I, determinando que os Comandos Conjuntos devem ser subordinados "ao Comandante Supremo [o Presidente da República], por meio do Ministro de Estado da Defesa" (Brasil-CN 2010). O mesmo artigo indica que um*

6 Em abril de 2018 a França comunicou que pretende seguir a Alemanha na criação de uma "quarta força" singular.

7 Popularmente usa-se a expressão "jabuticaba" para indicar algo que, como a própria fruta, só existe no Brasil.

comando somente se subordina a uma força singular se composto exclusivamente por integrantes daquela força (Brasil-CN 2010).

Além da incomum situação citada acima, temos uma outra característica singular. Dentro da estrutura do Exército, o ComDCiber está subordinado ao Departamento de Ciência e Tecnologia (DCT), um órgão eminentemente ligado à pesquisa e desenvolvimento tecnológico (Brasil-MD 2020a). Subordinado ao ComDCiber está o Centro de Defesa Cibernética (CDCiber), o qual é o responsável pela execução das operações cibernéticas, tanto ofensivas quanto defensivas. Por conseguinte, trata-se de um comando operacional vinculado a um órgão de ciência e tecnologia, o que constitui outra situação inusitada (Brasil-MD 2020a).

Na estrutura do ComDCiber encontramos, paralelamente ao CDCiber, o Estado-Maior Conjunto (EMC) e o Departamento de Gestão e Ensino (DGE). O ComDCiber é comandado por um General de Divisão (Oficial General de 3 estrelas). O CDCiber, o EMC e o DGP são comandados por Oficiais Generais de 2 estrelas. Sendo o Exército o responsável pelo setor cibernético, tanto o ComDCiber quanto o CDCiber são comandados apenas por militares desta força. Por conseguinte, a característica "conjunta" do comando limita-se à participação da Marinha e da Força Aérea no EMC e no DGE (Brasil-MD 2020a).

Há diversos problemas nessa opção brasileira. Primeiro, o Comandante do ComDCiber possui uma hierarquia relativamente baixa para as atividades que necessita desempenhar, tanto dentro do Exército, quanto no caso de operações conjuntas com as demais forças singulares, quanto em âmbito nacional. Há dificuldades no tocante à coordenação de ações, ou mesmo de discurso. Exemplo disso encontra-se na Estratégia Nacional de Defesa de 2016 que, embora reafirmando ser a defesa cibernética um setor estratégico sob responsabilidade do Exército (BRASIL, 2016, p. 31) dispõe também o que segue:

> Considerando que a **Força Aérea** se configura como uma **organização altamente tecnológica**, imprescindível se faz utilizar-se das capacidades de proteção dos Sistemas de Comando e Controle e **das Estruturas Estratégicas do País**, **principalmente daquelas que envolvam o espaço cibernético**. Deve, portanto, manter em elevado grau o nível de segurança e de defesa dos seus sistemas computacionais. (BRASIL, 2016, p. 30, grifos nossos)

A despeito de diversas críticas ao texto, inclusive deste autor, a nova versão da END 2020, enviada em julho ao Congresso Nacional para apreciação, manteve exatamente esse mesmo texto (Brasil-MD 2020b, 55).

Segundo, estando hierarquicamente numa posição muito baixa dentro do organograma do Exército, a disputa por orçamento fica bastante desequilibrada. Somente após a repartição do orçamento da defesa entre o MD e as forças singulares o ComDCiber terá seu orçamento determinado, dentre os diversos projetos prioritários do Exército. Mesmo sendo um comando operacional *de facto*, estando vinculado à área de C&T, a cultura nacional fará com que seja preterido na disputa por recursos com as áreas operacionais *de direito*. Exemplo disso é encontrado no Relatório do Senado Federal sobre a Política de Defesa Cibernética, onde se lê:

> Apresentamos sugestão de Emenda à Comissão de Relações e Defesa Nacional – CRE, no valor de R$ 60 milhões para a Defesa Cibernética, contudo a Comissão aprovou, **por escolha da Força** [o Exército Brasileiro], o Programa relativo à Aviação do Exército, como prioridade (Amin 2019, 56, grifo nosso).

Em outras palavras, o Exército Brasileiro preteriu o que a END estabelece como o setor estratégico atribuído a ele para destinar recursos à Aviação do Exército, que objetivaria assegurar o suprimento dos Pelotões de Fronteira, sob o argumento de que a Força Aérea não prioriza essa atividade (DefesaNet 2020a). Fosse essa uma prioridade da defesa nacional, seria mais sensato o MD realocar as prioridades da Força Aérea do que ins-

tituir uma Aviação de Asa Fixa no Exército. Destarte, o decreto autorizando a recriação da unidade de Aviação de Asa Fixa no Exército foi publicado em 02/06/2020, mas sob forte oposição da Força Aérea foi revogado no dia 08/06/2020 (DefesaNet 2020b). Logo, a Ciberdefesa, setor estratégico determinado pela END, perdeu os recursos para um projeto que não se concretizou.

Percebe-se, ainda, a ocorrência de dificuldades também no âmbito administrativo interno do próprio Exército, onde a cibernética aparenta ser uma atribuição intrínseca da Arma de Comunicações, de sorte que oficiais oriundos de outras armas têm dificuldades operacionais em serem aproveitados pelo ComDCiber. Ocorre que os *planos de carreira* das armas (Infantaria, Cavalaria, Artilharia, Engenharia, Comunicações, Intendência e Material Bélico, para citar as mais relevantes) exigem que os oficiais das mesmas passem por determinadas etapas ao longo de sua trajetória profissional. Outrossim, para que um oficial da arma de Infantaria possa galgar ao generalato, deverá forçosamente atuar em unidades e funções de infantaria por longos períodos, mesmo que se tenha identificado ou sobressaído, em determinado momento da carreira, em operações cibernéticas. Assim, recursos humanos importantes para a ciberdefesa, cujas habilidades dificilmente serão repostas, são remanejados para outras áreas por questões administrativas.

Outra dificuldade dessa vinculação histórica apresenta-se no tocante à já citada distribuição dos escassos recursos financeiros recebidos do Ministério da Defesa. Do quinhão recebido pelo Exército há uma subsequente disputa entre os projetos prioritários das diferentes armas. Até 2018 (10 anos após a END ter designado a ciberdefesa como setor estratégico da defesa nacional) todos os comandantes do ComDCiber eram oriundos da arma de Comunicações. Em todo esse período não houve no Alto Comando do Exército nenhum 4 Estrelas oriundo dessa arma. Tal situação talvez seja mitigada com a assunção do ComDCiber, por um oficial general oriundo da arma de Artilharia, em 2018.

Adicionalmente, dentre todas as nações analisadas, apenas o Brasil não dispõe de agência de Inteligência de Sinais (SIGINT), ainda que a mesma tenha sido recomendada pela CPI da Espionagem do Senado Federal instituída no rastro das denúncias de Snowden, em 2013 (BRASIL, 2013). Por conseguinte, a capacidade cibernética nacional fica ainda mais limitada, elevando a importância do ComDCiber e demandando maior agilidade e celeridade em sua completa operacionalização e efetividade.

Da Necessidade de Ampliação do Efetivo do ComDCiber

Quanto ao Tamanho do Efetivo Necessário

Segundo os poucos dados disponíveis, o efetivo do ComDCiber é de aproximadamente 180 pessoas. Por conseguinte, um efetivo menor que o de uma Companhia tradicional, mas com a responsabilidade operacional de uma Brigada, e comandado por um General de Divisão. Este efetivo é claramente inadequado para uma nação com as características econômicas, demográficas, geopolíticas, e mesmo militares, do Brasil.

Com base nos dados do Global Fire Power (GlobalFirepower.com 2020) de 2020 e da Tabela 1 pode-se tecer algumas análises.

Paridade de Poder de Compra (Purchase Parity Power) do PIB

A Tabela 2 apresenta uma amostra de países ordenada de acordo com seu PIB ajustado pela Paridade do Poder de Compra (PPC).

Tabela 2: População, Efetivos Militares e PIB (PPP) de diferentes países

EUA	População	Ativa	%Atv	PPP (bi USD)	Def. (bi USD)	%Def	IDA
China	1.384.688.986	2.183.000	0,16%	24.810	237	0,96%	6,06
EUA	329.256.465	1.400.000	0,43%	19.850	750	3,78%	8,89
Alemanha	80.457.737	182.650	0,23%	4.300	50	1,16%	5,12
Rússia	142.122.776	1.013.628	0,71%	4.025	48	1,19%	1,67
Brasil	208.846.892	334.500	0,16%	3.300	28	0,84%	5,26
Reino Unido	65.105.246	192.660	0,30%	2.974	55	1,85%	6,26
França	67.364.357	268.000	0,40%	2.904	42	1,43%	3,59
Itália	62.242.674	175.000	0,28%	2.344	28	1,19%	4,22

Fonte: Global Firepower Index 2020 (elaborada pelo autor)

Proporcionalidade do Efetivo Cibernético Quanto ao Efetivo Total

Conforme se observa, a China tem um PIB (PPP) de 24,81 trilhões de dólares, os EUA um de 19,85 trilhões de dólares, o Brasil de 3,30 trilhões e assim sucessivamente. O PIB-PPC do Brasil encontra-se 11% acima daquele do Reino Unido e 13% acima do da França. Logo, é presumível que tenhamos que defender interesses econômicos da mesma ordem de grandeza dos desses países. Isso estabelece um primeiro parâmetro de comparação da necessidade de força.

Tome-se agora a Tabela 3, que considera os dados dos efetivos militares de alguns desses países, complementados com dados dos respectivos efetivos militares de ciberdefesa tornados públicos. Cabe observar que a coluna CyberCom informa apenas os efetivos militares de cada país em seus comandos nacionais cibernéticos. Por conseguinte, não estão considerados os mais de 7.000 funcionários da NSA dos EUA, por se tratar da agência de inteligência de sinais. No caso britânico não foi considerado o Batalhão 77, por ser este dedicado a guerra informacional, tratada por este autor como um tema separado.

Tabela 3: Comparação dos efetivos de ciberdefesa e efetivos militares

País	Ativa	CyberCom	%Cib	%Méd	%UK	%FR	**%US**
EUA	1.400.000	6.200	0,44%	14.943	14.533	18.284	6.200
Brasil	334.500	180	0,05%	3.570	3.472	4.368	1.481
França	268.000	3.500	1,31%	2.861	2.782	3.500	1.187
Reino Unido	192.660	2.000	1,04%	2.056	2.000	2.516	853
Alemanha	182.650	13.500	7,39%	1.950	1.896	2.385	809
	2.377.810	25.380	1,07%				

Fonte: Elaborada pelo autor

Dentre os países apresentados na Tabela 3, depreende-se que os EUA são o país com o maior efetivo militar na ativa, com o Brasil em segundo, e assim por diante. Quando considerados os dados relativos ao pessoal engajado na ciberdefesa com relação ao efetivo total, coluna "%Cib", no entanto, o Brasil fica completamente fora do contexto dos demais países.

Em termos comparados, a Alemanha dispõe de uma força cibernética singular com efetivo equivalente a 7,39% do efetivo total de suas forças armadas. A França emprega 1,31% de seu efetivo total, e o Reino Unido 1,04%, enquanto os EUA têm 0,44% e Brasil apenas 0,05%. A média geral dos "efetivos cibernéticos" foi de 1,07% dos efetivos totais. Se considerado que o percentual médio consiste num quantitativo razoável, os efetivos nacionais deveriam ser aqueles da coluna "%Med". Se considerado o índice britânico, os dados seriam aqueles da coluna "%UK", pelo índice da França os da coluna "%FR" e pelo dos EUA aqueles da coluna "%US". Por esses dados, respectivamente, o efetivo da ciberdefesa brasileira deveria ser de 3.570, 3.472, 4.368 ou 1.481 profissionais, conforme o critério de ponderação escolhido, para a manutenção de um mínimo de proporcionalidade de forças de ciberdefesa com as desses países.

Não obstante, como já exposto, os interesses econômicos brasileiros são comparáveis àqueles franceses e britânicos (em verdade mais de 10% maiores). Logo, o efetivo comparável mais adequado para a ciberdefesa brasileira, incluindo militares, civis e terceirizados, deveria ser de 3.472, pela proporção britânica, ou 4.368 no caso francês, para a manutenção de um equilíbrio dos quantitativos de forças cibernéticas proporcionalmente ao restante das FAs. Embora os números possam parecer um tanto elevados, o maior deles corresponde aproximadamente ao efetivo de uma Brigada tradicional.

Pode-se concluir, por qualquer parâmetro analisado, que o efetivo do ComDCiber brasileiro é bastante diminuto, o que como visto não é explicável por nenhum parâmetro usual de comparação relativa: percentual do PIB empregado em Defesa; tamanho do efetivo militar total em relação ao tamanho da população, ou o tamanho do efetivo cibernético em relação ao tamanho do efetivo total. Uma explicação plausível é a da falta de uma maior conscientização dos riscos e dos prejuízos reais inerentes à falta de uma ciberdefesa compatível com os interesses envolvidos.

A justificativa da manutenção desse estado de coisas em geral é feita fundamentalmente sob o argumento de que não dispomos de recursos materiais e humanos, devido ao contingenciamento e aos cortes orçamentários, ou de que a Emenda Constitucional 95 (EC95) congelou as despesas governamentais nacionais até 2037. Ocorre que os países citados na comparação também enfrentam cortes orçamentários em suas áreas de defesa. As já citadas unidades do Cyber Mission Force dos EUA, anunciadas em 2014, foram completadas em maio de 2018, quatro meses antes do planejado. No entanto, entre 2014 e 2018 o orçamento do DoD foi reduzido em cerca de 8,5%, enquanto o orçamento do USCyberCom foi aumentado em 8%. Portanto, um crescimento proporcionalizado de mais de 18%, demonstrando que os EUA trabalham com uma priorização diferente para a ciberdefesa. Igualmente, os dados do Reino Unido e da Austrália demonstram essa priorização.

Da teoria da estratégia, sabe-se que na ausência de meios deve-se priorizar os fins buscados. A PND e a END determinam as supostas áreas prioritárias de cada força. A MB passa uma percepção de priorizar o PROSUB (submarino de propulsão nuclear) até mesmo sacrificando a manutenção da força de superfície. Mas o campo espacial pouco avança na FAB, assim como a cibernética no Exército.

Considerando-se a conclusão anterior de que os interesses brasileiros são da mesma ordem de grandeza

daqueles de Reino Unido e França, e seguindo a lógica de relativa proporcionalidade entre os efetivos militares e aqueles cibernéticos, o efetivo do ComDCiber deveria ser de ao menos 3.500 profissionais. No entanto, um crescimento dessa magnitude demanda tempo. Uma possibilidade ambiciosa, mas factível, seria um crescimento em oito anos, ou quatro fases de dois anos (tempo médio da troca do comandante de uma unidade militar). Atingir-se-ia o total 3.500 profissionais de acordo com a escala da Tabela 4.

Tabela 4: Proposta de Evolução do Efetivo do ComDCiber

Ano	Efetivo Inicial	1º Semestre	2º Semestre	Efetivo Final	**Crescimento**
2021	150	30	45	225	50%
2022	225	60	90	375	67%
2023	375	120	140	635	69%
2024	635	175	200	1010	59%
2025	1010	225	250	1485	47%
2026	1485	275	300	2060	39%
2027	2060	325	350	2735	33%
2028	2735	375	390	3500	28%

Fonte: Elaborada pelo autor

Esse crescimento escalonado prevê o recrutamento, seleção, absorção, treinamento e operacionalização do pessoal em todos os diferentes setores do ComDCiber, e prevê que conforme a estrutura cresça ela será tanto mais capaz de absorver maiores contingentes em termos absolutos, mas menores em termos relativos. Mas considera também a necessidade de um crescimento mais acelerado nas fases iniciais para buscar reduzir o gap hoje existente.

Da Necessidade de Pessoal Civil

É pacífico que o ciberdefesa deve envolver não apenas pessoal militar, mas também pessoal civil, em particular (mas não apenas) pela impossibilidade de se encontrar pessoal militar com a qualificação necessária nas quantidades necessárias exclusivamente nas fileiras das forças armadas. A principal discussão que se dá no âmbito dos EUA, Reino Unido, França e Alemanha é de como se captar e reter pessoal civil e usá-lo em operações militares. Alguns entendem que, estando a serviço da nação, e fora de uma zona de combate tradicional, há pouca diferença entre um militar uniformizado e um civil. Para estes, basta que se contratem civis diretamente nas forças armadas, até mesmo por contratação de empresas terceirizadas, para dispor do pessoal necessário, colocando-se em contrato as exigências de sigilo, hierarquia e disciplina (Paul, Porche, and Axelband 2014, 26–27; Bracknell 2018; Schneider 2018). Aqueles mais conservadores entendem que deve ser exigido o uso do uniforme, e do *ethos* militar, também dos "guerreiros" do domínio cibernético. Para a maioria destes, os profissionais de formação civil poderiam ser admitidos, mas na forma de oficiais temporários ou de carreiras auxiliares (Armstrong 2018). Uma questão relevante é a da existência de perspectivas de progressão de carreiras para o pessoal de cibernética. Isso já foi equacionado pelo US Army e pelos US Marines, que criaram carreiras específicas, assegurando a progressão profissional, embora se tenha consciência de que não serão carreiras de longa duração (Pomerleau 2018).

Comissionamento de Civis

Na página da Internet do US Army CyberCom existe uma inscrição on-line para pessoal com formação em programação, análise de sistemas ou *hacking* (U.S. Army Cyber n.d.). Outra página oferece a possibilidade de inscrição para candidatura ao comissionamento como oficiais do exército (U.S. Army Cyber n.d.). Sendo aceitos (após adequado processo de "investigação social" e comprovação da competência técnica), passam por um treinamento de apenas 6 semanas de instrução militar, e tornam-se oficiais do *U.S. Army CyberCom*. Similarmente, a USAF mantém uma página para o recrutamento de Cyberspace Operations Officers (U.S. Air Force n.d.) e a USNavy uma para o recrutamento de Cyber Warfare Engineers (U.S. Navy n.d.).

Embora essa não seja a forma ideal de recrutamento de civis, ela é facilmente adaptável ao caso brasileiro, onde também existe a provisão de ingresso regular de oficiais em carreiras diversas nas FAs. Cumpre ressaltar que o recrutamento não pode ser adstrito ao contexto tecnológico, mas deve necessariamente considerar a multidisciplinariedade da ciberdefesa, que para além de informática e engenharia eletrônica, compreende matemática, estatística, estudos de segurança e defesa, estudos estratégicos, relações internacionais, direito e ciência política, apenas para citar algumas. A remuneração do oficialato das forças armadas em 2020 corresponde ao indicado na Tabela 5. Observa-se que o soldo constitui a remuneração básica, sendo acrescido por gratificações, das quais as mais relevantes são o Adicional de Disponibilidade, "em razão da disponibilidade permanente e da dedicação exclusiva" e o Adicional de Habilitação, "em razão de cursos realizados com aproveitamento" na carreira (Brasil-CN 2019). O Adicional de Disponibilidade também é indicado na Tabela 5.

Tabela 5: Soldos Militares

Patente	Soldo (R$)	Adic. Dispon.
Capitão de Mar e Guerra e Coronel	11.451,00	32%
Capitão de Fragata e Tenente-Coronel	11.250,00	26%
Capitão de Corveta e Major	11.088,00	20%
Capitão-Tenente e Capitão	9.135,00	12%
Primeiro-Tenente	8.245,00	6%
Segundo-Tenente	7.490,00	5%

Fonte: Elaborada pelo autor com dados da Lei 13.954/2019 (Brasil-CN 2019)

Na Tabela 6 são encontrados os percentuais de Adicional de Habilitação de acordo com os cursos realizados, com os acréscimos anuais previstos em lei.

Tabela 6: Adicionais de Habilitação

Cursos	A partir de 01/07/2020	A partir de 01/07/2021	A partir de 01/07/2022	A partir de 01/07/2023
Altos Estudos - Categoria I	42%	54%	66%	73%
Altos Estudos - Categoria II	37%	49%	61%	68%
Aperfeiçoamento	27%	34%	41%	45%
Especialização	19%	22%	25%	27%
Formação	12%	12%	12%	12%

Fonte: Elaborada pelo autor com dados da Lei 13.954/2019 (Brasil-CN 2019)

Nessas condições, um analista de sistemas com formação em ciência da computação e com mestrado, que ingressasse na carreira na função de Segundo-Tenente em 2021, perceberia uma remuneração correspondendo ao soldo de R$ 7.490,00, acrescido de um Adicional de Disponibilidade de R$ 374,50 (5%) e de um Adicional de Habilitação de "Aperfeiçoamento" no valor de R$ 2.022,30 (27%), totalizando uma remuneração bruta de R$ 9886,80. O ingresso na mesma função nos anos subsequentes corresponde a um valor ainda maior, dado o aumento do Adicional de Habilitação programado para os próximos anos.

Nas condições de mercado brasileiras constitui-se uma remuneração bastante atrativa para profissionais de informática. O salário médio de mercado da categoria é bastante inferior, conforme se observa na Tabela 7.

Tabela 7: Remuneração Média de Analistas de Sistemas

Porte da Empresa	Nível Profissional				
	Trainee	Júnior	Pleno	Sênior	Master
Experiência (anos)	<3	3-4	5-6	7-8	>8
Pequena	R$ 2.492,81	R$ 3.116,01	R$ 3.895,01	R$ 4.868,76	R$ 6.085,95
Média	R$ 3.240,65	R$ 4.050,81	R$ 5.063,51	R$ 6.329,39	R$ 7.911,74
Grande	R$ 4.212,84	R$ 5.266,05	R$ 6.582,56	R$ 8.228,20	R$ 10.285,25

Fonte: Elaborada pelo autor com dados do TrabalhaBrasil (TrabalhaBrasil 2020)

Considerando-se o Exército como empresa de grande porte, claramente não haveria dificuldade na contratação até o nível de Analista Sênior (8 anos de experiência) equiparável a um Capitão, cuja remuneração bruta seria de R$ 12.697,45. Considerando-se ainda os demais benefícios proporcionados pela carreira militar (alimentação, transporte, plano de saúde, e possivelmente moradia), a atratividade é bastante elevada.

Ademais, ao Exército é facultada a "convocação e a incorporação de brasileiros com reconhecida competência técnico-profissional ou com notória cultura científica no serviço ativo do Exército, em caráter voluntário e temporário" (Brasil-CN 2018). Nessas condições a atratividade é ainda mais elevada. Comissionado como Major, um graduado em Ciência da Computação, com Doutorado, por exemplo, perceberia um Soldo de R$ 11.088,00, acrescido de Adicional de Disponibilidade de R$ 2.217,60 (20%) e de Adicional de Habilitação de R$ 4.656,96 (42%), totalizando uma remuneração bruta de R$ 17.962,56. Um valor 75% superior à média dos analistas de Sistemas Master (mais de 8 anos de experiência) em grandes empresas no mercado nacional.

A impossibilidade de ampliação do quadro de oficiais imposta pela EC95 não se constitui uma restrição *de facto*. Um reordenamento de prioridades permitiria o remanejamento de "postos" de Oficiais Técnicos Temporários (OTT) ou do Quadro Complementar de Oficiais (QCO) para o ComDCiber (a partir das três forças singulares). Os OTTs poderiam ser empregados em operações em curto espaço de tempo, e mesmo a limitação de oito anos de exercício permite um ciclo de vida razoavelmente longo na defesa. Findo o tempo de serviço, estes poderiam reforçar as fileiras da ciberdefesa e cibersegurança no mercado privado ou mesmo no setor público, continuando a contribuir com a ciberdefesa.

Cargos Civis

O comissionamento de civis é uma espécie de "conversão rápida" de civis em militares. Mas ele não inte-

ressará a um determinado conjunto de profissionais, os quais preferirão servir à ciberdefesa permanecendo em sua condição de civis, escapando às idiossincrasias do quotidiano militar, como marchas, formaturas, testes de aptidão física, uso de uniformes, etc. Além da ampliação do espectro de oferta de profissionais à disposição, a contratação de civis permitiria maior continuidade da retenção de conhecimentos associados à função, dado que os militares, por exigência da carreira, são frequentemente movimentados para a realização dos cursos e outras atividades. Os civis, isentos dessas obrigações, poderiam assegurar a estabilidade e continuidade dos processos.

Não obstante, é necessário que haja um plano de carreira que permita que os civis possam ascender inclusive a cargos de natureza decisória e de planejamento. Em termos técnicos isso não é um problema, mas em termos práticos essa convivência de militares e civis em funções equivalentes demandará uma adequação normativa (e principalmente cultural) das Forças Armadas. A possível criação de uma Carreira de Estado de Especialista em Defesa que agora aparece na END de 2020 pode ajudar a suprir essa lacuna (Brasil-MD 2020b, 43). Esse processo de integração civil-militar em ciberdefesa já ocorreu em outros países, sendo possível que o ComDCiber se beneficie das experiências de "nações amigas" nesse processo.

Criação de Uma Carreira Cibernética Militar

É necessária, a médio prazo, a criação de uma força cibernética singular. Entrementes, no curto prazo urge a criação de carreiras cibernética que permita a ascensão profissional dos militares oriundos das diferentes armas, nas diferentes forças singulares, que enveredarem por esse novo domínio, evitando que os mesmos tenham que ser afastados para servirem em postos e funções específicas de suas armas de origem. Os militares que ingressarem nessa "carreira" (ou quadro) apenas afastar-se-iam para os cursos de aperfeiçoamento, estado-maior e política e estratégia, a exemplo do que foi feito pelo U.S. Army e pelo U.S. Marine Corps.

Onde Alocar a Ciberdefesa Brasileira No Contexto do MD?

Urge também equacionar a subordinação do ComDCiber dentro da estrutura do MD. Duas alternativas são mais adequadas do que a atual vinculação ao DCT.

Alternativa 1 – Vinculação ao EMCFA

A proposta mais consistente, considerando-se as experiências dos países do "Arco do Conhecimento" militar, seria a da alocação do ComDCiber subordinado ao EMCFA, no MD. Essa opção elevaria o status da ciberdefesa, dado que esta deixaria de estar vinculada a uma força singular e tornar-se-ia, de fato, um comando conjunto subordinado ao EMCFA, mesmo que o comando seja permanentemente do Exército. Isso, em tese, permitiria maior facilidade na obtenção de recursos, incluindo o remanejamento de "vagas" de oficiais temporários e de quadros complementares junto às FAs, bem como facilitaria a obtenção de recursos, uma vez que reduziria dois "níveis" (entre as armas e entre os departamento do Exército) na disputa. Em termos práticos não deveria representar um problema para o Exército, posto que ele "perderia" a dotação orçamentária equivalente, mas também "perderia" a despesa correspondente, sem a perda do prestígio, pois permaneceria no comando por força da END. Constitui, assim, um "jogo de soma zero". Não obstante, tal opção pode enfrentar dificuldades de natureza política, dada a incipiente atuação conjunta do MD em seus 20 anos de existência, ainda mais cedo ou mais tarde essa atuação conjunta tenha que se tornar efetiva. Quanto antes,

melhor, e a crescente importância da cibernética no contexto militar internacional pode alavancar o desenvolvimento dessa capacidade de atuação conjunta.

Alternativa 2 – Adoção do Modelo do Comando e Operações Especiais (COpEsp)

Na impossibilidade de se dispor de uma estrutura diretamente vinculada ao EMCFA, uma alternativa dentro do próprio Exército seria dotar o ComDCiber de uma condição similar àquela do COpEsp. De fato, a natureza das operações cibernéticas é, em certa medida, "similar" àquela das operações especiais (Paul, Porche, and Axelband 2014). São, essencialmente, dois comandos operacionais. Ambos envolvem o desenvolvimento de doutrinas e técnicas específicas, distintas e complementares àquelas do restante do Exército, de sorte que podem dispor de "tratamento administrativo" similar.

Ainda que a solução adotada para o COpEsp possa parecer outra jabuticaba, ao menos seriam dois comandos que fariam uso da mesma exceção, e não duas exceções diferentes, uma para cada comando.

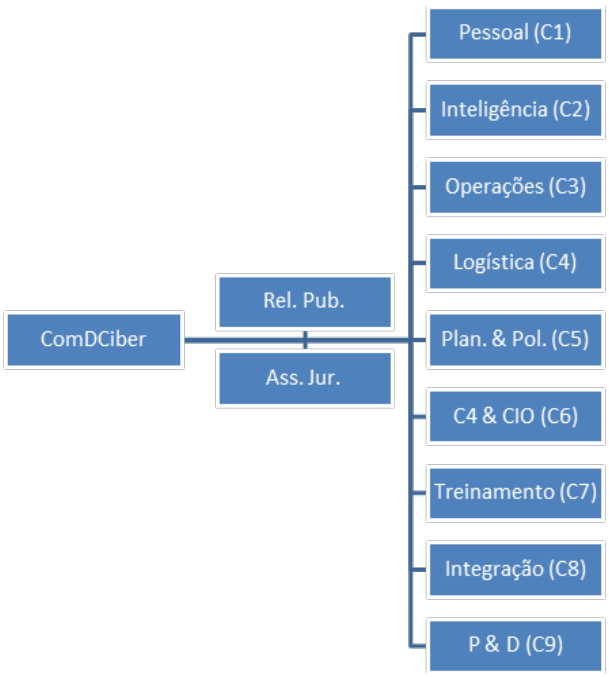
Da Estrutura e Funções do ComDCiber

Nesta seção avalia-se a necessidade de reestruturação do ComDCiber para contemplar as atividades desempenhadas por seus congêneres estrangeiros.

Reorganização das Responsabilidades do ComDCiber

O ComDCiber no Brasil deve ter responsabilidades similares àquelas de seus pares em outros países. O organograma proposto a seguir é funcional, representando as funções exercidas por congêneres do ComDCiber em outros países, e não necessariamente hierárquico. Dentro da lógica militar as funções podem ser rearranjadas em "subunidades" mais concentradas

Figura 2: Funções Necessárias à Ciberdefesa



Fonte: Elaborada pelo autor

Rel. Pub. (Relações Públicas)

A doutrina brasileira estabelece que segurança é uma sensação, uma percepção (Brasil-MD 2014). Portanto, faz-se necessária a divulgação organizada e concentrada de informações pertinentes. O controle da narrativa é parte essencial da chamada guerra informacional, a qual tem grande superfície de contato com a ciberdefesa. Por conseguinte, é necessária a existência de uma área de relações públicas para assessorar o Comandante e reforçar a percepção de segurança do público externo. Em conversas com militares com experiência no ComDCiber, observa-se que a lógica atual é a de se suprimir a divulgação de informações sobre a atuação do comando como forma de se evitar "provocar" ou "atiçar" os hackers, dado que os mesmos são movidos a desafios. Tal atitude, no máximo, seria plausível contra hacktivistas e hackers aventureiros, que atuem individualmente ou em pequenos grupos. Portanto, objetos de cibersegurança, e não ciberdefesa. Hackers patrocinados por estados, a razão de ser da ciberdefesa, têm alvos e estratégias bem definidos, contínuos e de longo prazo, como se observa nas atuações das APTs (*Advanced Persistent Threats*), e não são sujeitos a provocações. Por conseguinte, no caso do ComDCiber essa "estratégia do silencio" não faz sentido, reforçando a necessidade de um serviço efetivo (eficiente e eficaz) de relações públicas que venha a controlar a narrativa e o discurso da ciberdefesa brasileira.

Ass. Jur. (Assessoria Jurídica)

A legislação cibernética é nova em todo o mundo. Por conseguinte, não dispões de um amplo embasamento doutrinário e jurisprudencial consolidado. Nem no Brasil, nem no sistema internacional. É necessário dispor de uma assessoria jurídica que seja capaz de analisar os impactos legais específicos do tema para assessoramento do Comando.

É importante que esta assessoria disponha de capacidade de análise das propostas de normas nacionais e internacionais sobre o tema, para viabilizar o posicionamento do comando e do MD quanto aos acordos propostos. Esta assessoria também deve ter competência propositiva, no sentido de elaborar propostas de portarias ministeriais, decretos e mesmo de alterações na legislação a serem ofertadas ao Congresso visando a melhoria das capacidades cibernéticas nacionais.

Pessoal (C1)

A necessidade de pessoal para a ciberdefesa tende a ser crescente, sendo necessária a consolidação do planejamento e execução de políticas para aquisição e retenção de pessoal. Dada a necessidade de estabilidade do quadro de pessoal no médio e longo prazos, devido ao caráter de contínuo treinamento e aprendizado inerentes à área, deve-se atuar no *coaching* dos profissionais, bem como do monitoramento de metas e de políticas de segurança de acesso, sempre integrado às funções de C2 (Ciberinteligência). Esta função Deve também atuar em conjunto com a função C7 (Treinamento) de modo a fazer com que os profissionais do comando que venham a participar de eventos externos, e identifiquem talentos de potencial interesse para "recrutamento".

Juntamente à Assessoria Jurídica, esta função deverá buscar continuamente aprimorar os regulamentos das forças singulares no tocante à harmonização das carreiras dos profissionais oriundos das diferentes "armas" das forças, de forma a se evitar que os talentos em ciberdefesa e cibersegurança sejam dispersos a fim de não "sacrificarem" ou "comprometerem" suas carreiras nas respectivas "armas" de origem.

Inteligência (C2)

Essa função deve se ocupar da realização das atividades "usuais" de inteligência relativas ao pessoal do

Comando, principalmente no tocante à aquisição, distribuição e controle de conhecimento sigiloso. Igualmente, deve ocupar-se da contrainteligência.

Ela também deve interagir com as demais agências de inteligência nacionais e de nações amigas no intercâmbio de dados, informações, processos e tecnologias potencialmente relevantes.

Adicionalmente, deve monitorar as publicações de trabalhos de pós-graduação e artigos no ambiente acadêmico sobre o tema cibernético e correlatos, de forma a identificar não apenas potenciais talentos, mas também oportunidades e ameaças. No contexto destas, deve também monitorar o "mercado negro" de vulnerabilidades e armas cibernéticas.

Operações (C3)

Essa função ocupa-se das operações de Operações Cibernéticas (CNO), contemplando as operações de Exploração (CNE), Ofensivas ou de Ataque (CNA) e Defensivas (CND). Para tanto, engloba o projeto, especificação e apoio ao desenvolvimento de ferramentas de software que instrumentalizem essas operações.

É ela também que deve empreender as ações de inteligência planejadas por C2 (Inteligência) no âmbito cibernético, bem como validar os resultados obtidos.

Logística (C4)

À função Logística cumpre assegurar a disponibilidade de infraestrutura física e lógica do comando, incluindo a obtenção e gestão dos ativos de rede, bem como seu planejamento de capacidade e de instalações. Por conseguinte. É a responsável pelo planejamento e execução das aquisições. Dados os controles sobre as compras públicas, que geralmente implicam em longos ciclos de aquisição, e os geralmente longos prazos de desenvolvimento de software, esta função necessariamente deve trabalhar com um planejamento avançado em relação às demandas do comando.

Planejamento & Política (C5)

A essa função cumpre efetuar o planejamento e execução das políticas do Comando, e a coordenação com aquelas dos demais setores, acompanhando e atuando sore eventuais desvios. Sendo uma função de longo prazo, deve ter especial atenção à existência de uma equipe com longo ciclo de permanência, onde a participação de civis pode mostrar-se relevante para mitigar a rotatividade comum à carreira militar.

CIO (C6)

Similarmente à sua congênere no mundo civil, esta função ocupa-se de empreender o controle das atividades de gestão da informação, coordenando a integração das atividades de C2 (inteligência), C4 (Logística) e C5 (Planejamento & Política).

Treinamento (C7)

Essa função deve efetuar o planejamento e execução de treinamentos, workshops, congressos, exercícios e competições visando a qualificação do pessoal do Comando e de agências e instituições, públicas e privadas, de interesse da defesa nacional. É necessário que o escopo destes englobe não apenas exercícios de natureza técnica, como exercícios do tipo "capture a bandeira", mas também exercícios de natureza estratégica e político-militares (*Pol-Mil Games*), como no Caso do Exercício Guardião Cibernético, já com duas edições realizadas. No campo das competições acadêmicas, que permitem a identificação de talentos e de ideias inovadoras, o Atlantic Council promove, anualmente o exercício Cyber 9/12 Strategic Challenge[8], dentro da Cyber Sta-

8 https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/cyber-912/

tecraft Initiative, destinado a estudantes universitários da Europa e EUA, bem como de nações amigas, modelo que pode ser facilmente adaptado à realidade nacional. O exercício, inicialmente realizado em Genebra e Washington a partir de 2015, hoje ocorre em diversas sedes: Genebra (Suíça), Washington, Nova Iorque, Austin (EUA), Londres (Reino Unido), Lille (França) e Camberra (Austrália).

Integração (C8)

A ciberdefesa militar é fundamentalmente dependente da melhoria das condições de ciberdefesa da sociedade como um todo. Portanto, é necessária a integração do ComDCiber com instituições públicas e privadas, e com o próprio cidadão comum.

Um bom exemplo é o do *National Cyber Security Centre* (NCSC) do GCHQ britânico, que busca fomentar a defesa cibernética com a geração de cartilhas e orientações de melhores práticas publicadas em seu próprio site, abertas ao público em geral e às empresas, bem como com a realização de treinamentos de agentes de cibersegurança e ciberdefesa de instituições públicas e privadas, e palestras e workshops em universidades britânicas.

Outra atividade deve ser a de interagir com os legisladores para a proposição de medidas que possam incrementar a defesa cibernética pública e privada. Exemplificando, EUA, Reino Unido e União europeia aprovaram legislações instituindo multas para concessionárias de serviços públicos vitimadas por ciberataques que não tivessem defesas ou resiliência para reduzirem seu impacto.

Na ausência de uma agência brasileira de SIGINT, pode ainda atuar junto à indústria nacional (e internacional) de software e hardware para a certificação de produtos de cibersegurança e ciberdefesa, e da própria cadeia produtiva. No Reino Unido o NCSC faz a certificação de produtos e serviços de cibersegurança para empresas (NCSC n.d.). Na França esse serviço é prestado pela Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) (ANSSI n.d.).

P & D – Pesquisa e Desenvolvimento (C9)

Esta função deve atuar em conjunto com a academia, departamentos de P&D de empresas e *think tanks*, para a criação de tecnologia e conhecimento nacionais que possam incrementar a ciberdefesa nacional. A ela cabe também fomentar a criação de cursos acadêmicos em universidades nacionais relacionados à ciberdefesa, nas diversas áreas do conhecimento anteriormente citadas. Adicionalmente, deve promover concursos de teses e artigos e, em conjunto com C7 (Treinamento), promover exercícios externos, para a identificação de novas técnicas e também de novos talentos.

Conclusão

O ciberespaço, inequivocamente, apresenta-se como um novo espaço de coerção interestatal. Mesmo países com uma cultura e tradição não-agressiva, que privilegiem a resolução pacífica de controvérsias, e se disponham a abrir mão das vantagens competitivas potencialmente oferecidas pelas potencialidades ofensivas do ciberespaço, não podem alimentar a expectativa de que seus pares façam o mesmo.

A ação estatal no ciberespaço é real, acontece diariamente, envolve interesses econômicos, estratégicos e geopolíticos de monta, é global, ignora o campo de batalha tradicional e é crescente. Muitas nações já atuam diuturnamente, enquanto ampliam seus conhecimentos, arsenais e amparo legal.

O Brasil necessita estar adequadamente preparado o quanto antes, e a constatação da pesquisa realizada mostra que os avanços do Brasil nesse domínio são por

demais lentos quando comparados aos de nações com interesses econômicos e geopolíticos do mesmo porte, e mesmo aos de "potências menores" como Austrália, Israel, Irã e Coreia do Norte.

Isso foi demonstrado por meio de uma análise comparada da ciberdefesa em diferentes países, retratando o descompasso da realidade brasileira. Mostrou-se as fragilidades das idiossincrasias das opções brasileiras por um 'comando conjunto' subordinado a uma força armada singular e por uma ciberestratégia que, depois de 10 anos da criação do ComDCiber, focou apenas na cibersegurança, relegando a ciberdefesa para um momento posterior. Foram abordadas questões como os tamanhos dos efetivos militares alocados, a necessidade de envolvimento pessoal civil multidisciplinar, e questões orçamentárias. Indo além da problematização, buscou-se a apresentação de propostas destinadas a sanar algumas das questões, de forma a permitir a abertura de um debate público sobre tema tão relevante para a sociedade e o Estado brasileiros.

As conclusões e proposições deste trabalho não são de caráter conclusivo, mas apontam um caminho coerente, baseado nos dados e conceitos apresentados, coletados em uma ampla pesquisa sobre as práticas de diversos países, de forma a proporcionar uma abordagem científica sobre este tema de caráter tão controverso quanto atual.

REFERÊNCIAS BIBLIOGRÁFICAS

Amin, Espiridião. 2019. "Relatório de Avaliação de Política Pública: A Política Nacional Sobre Defesa Cibernética." Brasília.

ANSSI. n.d. "Security Visa | Agence Nationale de La Sécurité Des Systèmes d'information." ANSSI Website. Accessed August 16, 2020. https://www.ssi.gouv.fr/en/security-visa/.

Armstrong, James. 2018. "The US Military Can't Just 'Hire' Cyber Expertise. Here's Why." Modern War Institute. May 2, 2018. https://mwi.usma.edu/us-military-cant-just-hire-cyber-expertise-heres/.

Auchard, Eric, and Jim Finkle. 2016. "Ukraine Utility Cyber Attack Wider than Reported." *Reuters*, 2016. http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UI23S20160104.

Australia. 2020. "Australia's Cyber Security Strategy 2020."

Bardin, Laurence. 2016. *Análise de Conteúdo*. São Paulo: Edições 70.

Barlouet, Alain. 2016. "La France Muscle Sa Cyberdéfense." *Le Figaro*, December 13, 2016.

Beaufre, André. 1998. *Introdução à Estratégia*. 1st ed. Rio de Janeiro: Biblioteca do Exército Editora.

Bracknell, Butch. 2018. "Who Says Cyber Warriors Need to Wear a Uniform?" Modern War Institute. March 23, 2018. https://mwi.usma.edu/says-cyber-warriors-need-wear-uniform/.

Brangetto, Pascal. 2015. *National Cyber Security Organisation: France*.

Brasil-CN. 2010. *Lei Complementar 136*. Brasília: Congresso Nacional.

———. 2014. "Relatório Da CPI Da Espionagem Eletrônica Do Senado Federal." Brasília, Brasil.

———. 2018. *Decreto 9.637/2019*. Brasília: Presidência da República.

———. 2019. *Lei 13.954/2019*. Brasília: Congresso Nacional. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13954.htm.

Brasil-GSI. 2018. *Política Nacional de Segurança Da Informação*. Brasília: Presidência da República.

———. 2020. "Estratégia Nacional de Segurança Cibernética." Brasília.

Brasil-MD. 2014. *Manual Básico Vol. 1*. Rio de Janeiro: ESG.

———. 2020a. "Exército Brasileiro - Organograma." Exército Brasileiro - Organograma. 2020. http://www.eb.mil.br/organograma.

———. 2020b. "Política Nacional de Defesa e Estratégia Nacional de Defesa." Brasília.

Breene, Keith. 2016. "Who Are the Cyberwar Superpowers? | World Economic Forum." World Economic Forum. May 4, 2016. https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers.

Clarke, Richard A, and Robert K Knake. 2010. *Cyber War: The next Threat to National Security and What to Do about It*. New York: HarperCollins Publishers.

DefesaNet. 2020a. "Aviação Do Exército - Exército Recria Aviação de Asas Fixas e FAB Critica." *DefesaNet*, June 6, 2020. https://www.defesanet.com.br/avex/noticia/37078/Exercito-recria-aviacao-de-asas-fixas-e-FAB-critica/.

———. 2020b. "Aviação Do Exército - Urgente - Revogado Decreto Sobe a Aviação Do Exército." *DefesaNet*, June 8, 2020. https://www.defesanet.com.br/avex/noticia/37089/Urgente---Revogado-Decreto-sobe-a-Aviacao-do-Exercito/.

Dragos. 2017. "CRASHOVERRIDE: Analyzing the Threat to Electric Grid Operations." https://dragos.com/blog/crashoverride/CrashOverride-01.pdf.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. 2011. "W32.Stuxnet Dossier." *Symantec-Security Response*. Vol. Version 1. https://doi.org/20 September 2015.

GCHQ. 2016. "GCHQ History." http://www.gchq.gov.uk/history/Pages/index.aspx.

GlobalFirepower.com. 2020. "2020 Military Strength Ranking." Global Firepower Index. 2020. https://www.globalfirepower.com/countries-listing.asp.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. Penguin Books.

Hayden, Michael V. 2016. *Playing to the Edge: American Intelligence in the Age of Terror*. New York: The Penguin Press.

Haynes, Deborah. 2018. "Britain to Create 2,000-Strong Cyber Force to Tackle Russia Threat | UK News | Sky News." *SkyNews*, September 21, 2018. https://news.sky.com/story/britain-to-create-2-000-strong-cyber-force-to-tackle-russia-threat-11503653.

IMF. 2019. "World Economic Outlook Database." World Economic Outlook Database. 2019. https://www.imf.org/external/pubs/ft/weo/2019/02/weodata/weorept.aspx?pr.x=57&pr.y=17&sy=2019&ey=2019&scsm=1&ssd=1&sort=country&ds=.&br=1&c=512%2C668%2C914%2C672%2C612%2C946%2C614%2C137%2C311%2C546%2C213%2C674%2C911%2C676%2C314%2C548%2C193%2C556%2C122%2C6.

Langner, Ralph. 2011. *Cracking Stuxnet, a 21st-Century Cyber Weapon*. TED Talks.

Malagutti, Marcelo. 2016. "State-Sponsored Cyber-Offences." *Revista Da Escola de Guerra Naval* 22 (2): 261–90. https://doi.org/10.21544/1809-3191/regn.v22n2p261-290.

———. 2017. "Statecraft within Cyberspace." *Cyber World Magazine*, December 2017.

Mandarino, Raphael, and Claudia Canongia. 2010. *Livro Verde Segurança Cibernética No Brasil. Gabinete de Segurança Institucional, Departamento de Segurança Da Informação e Comunicações; Organização Claudia Canongia e Raphael Mandarino Junior*. http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf.

Marks, Joseph. 2017. "At 7 Years Old, CYBERCOM Becomes a Full Combatant Command - Defense One." *Defense One*, August 17, 2017. https://www.defenseone.com/threats/2017/08/7-years-old-cybercom-becomes-full-combatant-command/140345/.

Moreira, José de Albuquerque. 1995. "Informática: O Mito Política Nacional de Informática." *Revista de Biblioteconomia de Brasília* 19 (1): 23–50.

NCSC. n.d. "NCSC Certification." NCSC Website. Accessed August 16, 2020. https://www.ncsc.gov.uk/section/products-services/ncsc-certification.

Osborne, George. 2015. "Chancellor's Speech to GCHQ on Cyber Security." *Gov.Uk*, 1–12. https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

Osula, Anna-Maria. 2015. *National Cyber Security Organisation: United Kingdom*.

Paganini, Pierluigi. 2015. "The British Army Creates the 77th Battalion." *Security Affairs*, February 15, 2015. https://securityaffairs.co/wordpress/33552/social-networks/british-army-77th-battalion-facebook.html.

Parlamento Europeu. 2018. "RELATÓRIO Sobre Ciberdefesa (2018/2004(INI)) - A8-0189/2018."

Paul, Christopher, Isaac Porche, and Elliot Axelband. 2014. "Cyber Forces and U.S. Cyber Command." In *The Other Quiet Professionals*. RAND Corporation. https://doi.org/10.4135/9781452229300.n1568.

Pernik, Piret, Jesse Wojtkowiak, and Alexander Verschoor-Kirss. 2016. *National Cyber Security Organisation: UNITED STATES*.

Pomerleau, Mark. 2018. "Why a Long Military Career in Cyber Feels like a Rarity." *FifthDomain*, September 18, 2018. https://www.fifthdomain.com/dod/2018/09/18/why-a-long-military-career-in-cyber-feels-like-a-rarity/.

Raud, Mikk. 2016. *China and Cyber: Attitudes, Strategies, Organisation*. NATO CCDCOE.

Rid, Thomas. 2016. *Rise of the Machines*. London: Scribe Publications.

Rosenzweig, Paul. 2013. *Cyber Warfare. Cyber Warfare*. Santa Barbara: Praeger. https://doi.org/10.1016/B978-0-12-416672-1.00013-1.

Rugge, Fabio. 2018. "Confronting an 'Axis of Cyber'?" Milano. https://www.ispionline.it/it/pubblicazione/confronting-axis-cyber-21458.

Rusbridger, Alan. 2013. "The Snowden Leaks and the Public." *The New York Review of Books*, November 21, 2013.

Sabbagh, Dan. 2020. "UK to Launch Specialist Cyber Force Able to Target Terror Groups." *The Guardian*, February 27, 2020. https://www.theguardian.com/technology/2020/feb/27/uk-to-launch-specialist-cyber-force-able-to-target-terror-groups.

Sanger, David E, and Eric Schmitt. 2014. "Snowden Used Low Cost Tool to Best NSA." *The New York Times*, February 8, 2014.

Schneider, Jacquelyn. 2018. "Blue Hair In The Gray Zone." *War On The Rocks*, January 2018.

Schulte, Sebastian. 2017. "German Cyber Command Becomes Operational." *Jane's*, no. 06 abr.

Segal, Adam. 2016. *The Hacked World Order*. Public Affairs.

Stokes, Mark. 2015. "The PLA General Staff Department Third Department Second Bureau."

TrabalhaBrasil. 2020. "Salario Para Analista de Sistemas. Media Salarial Paga No Brasil | Trabalha Brasil." TrabalhaBrasil.Com.Br. 2020. https://www.trabalhabrasil.com.br/media-salarial-para-analista-de-sistemas.

U.S. Air Force. n.d. "U.S. Air Force - Career Detail - Cyberspace Operations Officer." Airforce.Com. Accessed August 16, 2020. https://www.airforce.com/careers/detail/cyberspace-operations-officer.

U.S. Army Cyber. n.d. "Careers in Army Cyber." Goarmy.Com. Accessed August 16, 2020a. https://www.goarmy.com/army-cyber/careers-in-army-cyber.html.

———. n.d. "Cyber Direct Commissioning Program." Goarmy.Com. Accessed August 16, 2020b. https://www.goarmy.com/army-cyber/cyber-direct-commissioning-program.html.

U.S. ArmyCyber. 2020. "DOD FACT SHEET: Cyber Mission Force > U.S. Army Cyber Command > Fact Sheets." U.S. Army Cyber Command. February 10, 2020. https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/.

U.S. Navy. n.d. "Navy Cyber Warfare Engineer Officer Program." NavyCyberSpace (Navycs.Com). Accessed August 16, 2020. https://www.navycs.com/officer/cyberwarfareengineer.html.

United Kingdom. 2016. "Cyber Security Strategy." http://www.gov.uk/government/publications/cyber-security-strategy.

Voo, Julia, Irfan Hemani, Simon Jones, Winnona Desombre, and Daniel Cassidy. 2020. "National Cyber Power Index 2020 Methodology and Analytical Considerations." www.belfercenter.org/CCPI.

Wilentz, Sean. 2014. "Would You Feel Differently about Snowden, Greenwald, and Assange If You Knew What They Really Thought?" *New Republic*, January 19, 2014.

Zetter, Kim. 2011. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired*, July 2011. https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

———. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Random House USA.

———. 2016. "Everything We Know About Ukraine's Power Plant Hack." *Wired*, January 2016. https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.