HM Government

ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA 2016-2021

Sumário

APRESENTAÇÃO **4**

PREFÁCIO **5**

1. SUMÁRIO EXECUTIVO **6**

2. INTRODUÇÃO **8**

ESCOPO DA ESTRATÉGIA 9

3. CONTEXTO ESTRATÉGICO **10**

AMEAÇAS 10

Cibercriminosos 10

Estados e ameaças patrocinadas por Estados 11

Terroristas 11

Hacktivistas 12

"Script Kiddies" 12

VULNERABILIDADES 14

Um leque cada vez mais variado de dispositivos conectados 14

Falta de higiene cibernética e cumprimento de normas 14

Falta de capacitação e conhecimentos 14

Sistemas legados sem *patch* de correção 15

Disponibilidade de recursos de *hacking* 15

CONCLUSÕES 15

4. NOSSA RESPOSTA NACIONAL **16**

NOSSA VISÃO 16

PRINCÍPIOS 16

ATRIBUIÇÕES E RESPONSABILIDADES 17

Indivíduos ..... **Error! Bookmark not defined.**

Empresas e organizações 17

Governo 17

Promovendo a transformação: o papel do mercado 17

Promovendo a transformação: um papel mais amplo para o governo 18

PLANO DE IMPLEMENTAÇÃO **21**

5. DEFENDER 22

5.1. DEFESA CIBERNÉTICA ATIVA 22

5.2. CONSTRUÇÃO DE UMA INTERNET MAIS SEGURA 24

5.3. PROTEÇÃO AO GOVERNO 25

5.4. PROTEÇÃO ÀS INFRAESTRUTURAS CRÍTICAS NACIONAIS E OUTROS SETORES PRIORITÁRIOS 27

5.5. MUDANÇA DE COMPORTAMENTO NA POPULAÇÃO E NAS EMPRESAS 29

5.6. TRATANDO DE INCIDENTES E ENTENDENDO A AMEAÇA 32

6. DISSUADIR 34

6.1. O PAPEL CIBERNÉTICO NA DISSUASÃO 34

6.2. REDUÇÃO DA CRIMINALIDADE CIBERNÉTICA 34

6.3. COMBATE A ATORES ESTRANGEIROS HOSTIS 36

6.4. PREVINIENDO TERRORISMO 37

6.5. AUMENTO DA CAPACIDADE SOBERANA – CAPACIDADE CIBERNÉTICA OFENSIVA 37

6.6. AUMENTO DA CAPACIDADE SOBERANA – CRIPTOGRAFIA 38

7. DESENVOLVER 40

7.1. FORTALECIMENTO DA CAPACITAÇÃO EM SEGURANÇA CIBERNÉTICA 40

7.2. ESTÍMULO AO CRESCIMENTO NO SETOR DE SEGURANÇA CIBERNÉTICA 42

7.3. PROMOÇÃO DA CIÊNCIA E DA TECNOLOGIA DE SEGURANÇA CIBERNÉTICA 43

7.4. MONITORAMENTO EFETIVO DO HORIZONTE 45

8. AÇÃO INTERNACIONAL 47

9. INDICADORES 49

10. CONCLUSÃO: SEGURANÇA CIBERNÉTICA ALÉM DE 2021 51

ANEXO 1: SIGLAS 52

ANEXO 2: GLOSSÁRIO 53

ANEXO 3: SÍNTESE DO PROGRAMA DE IMPLEMENTAÇÃO 57

APRESENTAÇÃO

O Reino Unido está entre os países mais digitalizados do mundo. Atualmente, nossa prosperidade depende, em grande medida, da capacidade de proteger as nossas tecnologias, dados e redes contra uma infinidade de ameaças.

Todavia, os ataques cibernéticos estão cada vez mais frequentes, sofisticados e prejudiciais quando bem-sucedidos. Por isso estamos tomando ações decisivas para proteger tanto a nossa economia quanto a privacidade de nossos cidadãos.

Nossa Estratégia Nacional de Segurança Cibernética traça um plano para que a Grã-Bretanha se torne um país confiante, capaz e resiliente em um mundo digital em rápida evolução.

Ao longo de um horizonte de cinco anos, será investido £ 1,9 bilhão na defesa dos nossos sistemas e infraestruturas, na dissuasão dos nossos adversários e na capacitação de toda a sociedade – desde as maiores empresas até o cidadão.

Desde as noções mais básicas de higiene cibernética até medidas sofisticadas de dissuasão, nossa resposta tem de ser abrangente.

Concentraremos nossos esforços em elevar a onerosidade para quem promover ataques contra qualquer pessoa no Reino Unido, com defesas mais robustas e maior *know-how* cibernético. Já não é uma preocupação apenas da área de TI, mas de todos. O conhecimento cibernético deve permear todas as profissões.

O novo Centro Nacional de Segurança Cibernética será responsável por facilitar o acesso aos mais avançados conhecimentos técnicos em linguagem acessível para pessoas jurídicas e físicas, além de garantir uma rápida resposta a incidentes cibernéticos de grande escala.

Ainda que o governo assuma um evidente protagonismo no tema, também criaremos um ecossistema mais amplo que abranja o setor privado, reconhecendo as áreas em que este é mais capaz de inovar com maior agilidade. Haverá, ainda, um esforço para direcionar jovens mentes promissoras ao mundo da segurança cibernética.

A ameaça cibernética afeta toda a sociedade e, por isso, queremos ressaltar que todos terão um papel a desempenhar em nossa resposta nacional. É por isso que esta estratégia representa um exercício inédito de transparência. O debate do tema não pode mais continuar a portas fechadas.

A verdade é que a ameaça cibernética não pode ser completamente eliminada. A tecnologia digital somente funciona por ser aberta, e essa abertura traz consigo um risco. O que podemos fazer é reduzir a ameaça a um nível que garanta a nossa permanência na vanguarda da revolução digital. Esta estratégia traça o caminho nesse sentido.

Philip Hammond,
Ministro da Fazenda

PREFÁCIO

Nossa principal responsabilidade é com a segurança da nação e com a competência do governo, deveres estes que se refletem nesta estratégia. Trata-se de um plano arrojado e ambicioso para enfrentar as muitas ameaças que o nosso país enfrenta no ciberespaço. O controle e a mitigação dessas ameaças são uma tarefa de todos, mas o governo reconhece sua responsabilidade maior em coordenar o esforço nacional necessário.

O governo está empenhado em assegurar que os compromissos assumidos nesta estratégia sejam cumpridos e que o progresso dos avanços alcançados seja rigorosamente acompanhado e comunicado. Nossa metodologia estará sob constante reavaliação, acompanhando as mudanças no nível das ameaças enfrentadas e a evolução tecnológica em segurança.

O governo também tem uma responsabilidade especial para com a população, com as empresas e organizações atuantes no Reino Unido e com os nossos aliados e parceiros internacionais. Devemos estar em condições de garantir que foram envidados todos os esforços para manter a segurança de nossos sistemas e proteção de nossos dados e redes contra ataques ou interferências. Para isso, é preciso estabelecer os mais elevados padrões de segurança cibernética e assegurar o seu cumprimento, servindo estes como alicerce da segurança nacional e do bem-estar econômico do país, e como exemplo a ser seguido. Serão publicados relatos anuais dos avanços alcançados.

Como Ministro do Gabinete, responsável pela segurança cibernética e governamental, estou determinado a conduzir esta estratégia até sua consolidação. Atuarei em estreita articulação com outros integrantes do governo central e das administrações regionais, do setor público mais amplamente, do setor privado e do meio acadêmico, a fim de concretizar essa ambição.

Ben Gummer,
Ministro do Gabinete e Tesoureiro-Mor

1. SUMÁRIO EXECUTIVO

1.1. A segurança e a prosperidade do Reino Unido no futuro se sustentam em bases digitais. O desafio da nossa geração consiste na construção de uma sociedade digital ao mesmo tempo próspera e resiliente às ameaças cibernéticas e munida dos conhecimentos e das estruturas necessárias para maximizar as oportunidades e controlar os riscos.

1.2. O Reino Unido é fundamentalmente dependente da Internet. O meio, no entanto, é inerentemente inseguro e haverá tentativas constantes de explorar suas fraquezas para lançar ataques cibernéticos. É uma ameaça que não pode ser completamente eliminada, mas é possível reduzir o risco a um nível que permita à sociedade continuar a prosperar e obter benefícios das extensas oportunidades oferecidas pela tecnologia digital.

1.3. A Estratégia Nacional de Segurança Cibernética de 2011, vinculado ao Programa Nacional de Segurança Cibernética do governo do Reino Unido, orçado em £ 860 milhões, já propiciou melhorias substanciais à segurança cibernética no Reino Unido. Obteve resultados importantes em recorrer ao mercado para difundir comportamentos corretos de segurança cibernética. Contudo, essa abordagem ainda não alcançou a dimensão nem proporcionou a agilidade necessárias para se manter à frente das ameaças em rápida evolução. Agora, é preciso ir além.

1.4. Nossa visão para 2021 é que o **Reino Unido seja um país seguro e resiliente às ameaças cibernéticas, próspero e confiante no mundo digital**.

1.5. Para concretizar esta visão, teremos como objetivos:

• **DEFENDER** Devemos dispor dos meios para defender o Reino Unido contra a evolução das ameaças cibernéticas, para responder com eficácia à ocorrência de incidentes e para garantir que as redes, dados e sistemas do país sejam seguros e resilientes. A população, as empresas e o setor público devem ter os conhecimentos e a capacidade de se defenderem.

• **DISSUADIR** O Reino Unido não será alvo fácil para qualquer forma de agressão no ciberespaço. Devemos detectar, entender, investigar e frustrar as ações hostis empreendidas contra o país, perseguindo e levando a juízo os infratores. Devemos dispor de meios para promover ações ofensivas no ciberespaço, se assim optarmos.

• **DESENVOLVER** Devemos dispor de uma indústria de segurança cibernética inovadora e em expansão, apoiada por pesquisa e produção científica de ponta. Teremos uma safra autossustentável de talentos com conhecimentos que atendam às necessidades nacionais nos setores público e privado. Nossas análises e conhecimentos avançados permitirão ao país enfrentar e superar as ameaças e desafios futuros.

1.6. Em busca desses objetivos, empreenderemos **AÇÕES INTERNACIONAIS** e exerceremos a nossa influência através do investimento em parcerias que conduzam a evolução global do ciberespaço ao encontro dos nossos interesses econômicos e de segurança. Aprofundaremos as relações existentes com parceiros internacionais mais próximos, reconhecendo sua contribuição para o aumento da nossa segurança coletiva. Também formaremos laços com novos parceiros, contribuindo para a elevação de seus níveis de segurança cibernética e para a defesa dos interesses do Reino Unido no exterior. Essa atuação ocorrerá tanto de forma bilateral quanto multilateral, inclusive através da UE, da OTAN e da ONU. Enviaremos mensagens claras aos nossos adversários sobre as consequências reservadas a quem ameaçar causar prejuízo aos nossos interesses ou dos nossos aliados no ciberespaço.

1.7. Para alcançar estes resultados ao longo dos próximos cinco anos, o governo do Reino Unido pretende intervir mais ativamente e ampliar os investimentos, ao mesmo tempo mantendo o apoio às forças do mercado para elevar os padrões de segurança cibernética em todo o país. O governo, em parceria com as Administrações Regionais da Escócia, País de Gales e Irlanda do

Norte, trabalhará com os setores público e privado para garantir que a população, as empresas e entidades da sociedade civil adotem os comportamentos necessários à sua segurança virtual. Adotaremos políticas de intervenção (sempre que necessário e no âmbito das nossas competências) para promover melhorias que sejam do interesse nacional, sobretudo em relação à segurança cibernética das infraestruturas críticas nacionais.

1.8. O governo britânico utilizará seus recursos e os da iniciativa privada para desenvolver e aplicar medidas de defesa cibernética ativa[1], elevando significativamente os níveis de segurança cibernética nas redes do país. Dentre essas medidas estão a minimização das formas mais comuns de ataques de *phishing*, a filtragem de endereços IP infratores e o bloqueio ativo de atividades virtuais maliciosas. Essas melhorias na segurança cibernética básica servirão para reforçar a resiliência do Reino Unido às ameaças cibernéticas mais comuns.

1.9. Criamos o Centro Nacional de Segurança Cibernética (*National Cyber Security Centre – NCSC*) para atuar como referência em segurança cibernética do país, compartilhando conhecimentos, tratando de vulnerabilidades sistêmicas e exercendo liderança em questões-chave para a segurança cibernética nacional.

1.10. Asseguraremos que nossas Forças Armadas sejam resilientes e contem com defesas cibernéticas robustas o suficiente para proteger e defender suas redes e plataformas, mantendo a continuidade operacional e a liberdade de manobra em âmbito mundial, diante das ameaças cibernéticas. O Centro de Operações de Segurança Cibernética militar atuará em estreita articulação com o NCSC, podendo as Forças Armadas oferecer assistência em caso de um ataque cibernético nacional de grande escala.

1.11. Teremos meios de responder aos ataques cibernéticos da mesma forma que respondemos a qualquer outro ataque, utilizando-se os recursos considerados mais convenientes ao fim, inclusive ações cibernéticas ofensivas.

1.12. Utilizaremos a autoridade e a influência do governo para investir em programas destinados a combater a escassez de mão de obra qualificada em segurança cibernética no Reino Unido, abrangendo desde escolas até universidades e todo o mercado de trabalho do país.

1.13. Serão lançados dois novos centros de inovação cibernética para impulsionar o desenvolvimento de produtos cibernéticos de ponta e novas empresas dinâmicas de segurança cibernética. Também será destinada uma parcela dos £ 165 milhões do Fundo de Defesa e Inovação Cibernética (*Defence and Cyber Innovation Fund*) para financiar a contratação de produtos e serviços inovadores em defesa e segurança.

1.14. Será investido um total de £ 1,9 bilhão nos próximos cinco anos para revolucionar significativamente a segurança cibernética do Reino Unido.

[1] Entender as ameaças às redes para então formular e implementar medidas proativas de combate ou defesa dessas ameaças. Para uma explicação de todos os termos técnicos, consulte a seção Glossário.

2. INTRODUÇÃO

2.1. As tecnologias da informação e comunicação evoluíram ao longo das duas últimas décadas, passando hoje a integrar praticamente todos os aspectos de nossas vidas. O Reino Unido é uma sociedade digitalizada, o que enriquece a nossa economia e o nosso cotidiano.

2.2. A transformação gerada por essa digitalização gera novas dependências. Nossa economia, a administração pública e a garantia de serviços essenciais passaram a depender da integridade do ciberespaço e das infraestruturas, sistemas e dados que a sustentam. A perda da confiança pública nessa integridade comprometeria os benefícios dessa revolução tecnológica.

2.3. Grande parte dos *hardwares* e *softwares* originalmente desenvolvidos para viabilizar este ambiente digital interconectado priorizou a eficiência, o custo e a conveniência ao usuário, mas nem sempre teve em conta a segurança desde sua concepção. Agentes maliciosos, ou seja, Estados hostis, organizações criminosas ou terroristas e indivíduos, podem explorar essa brecha deixada entre a conveniência e segurança. Sanar essas deficiências é hoje uma prioridade nacional.

2.4. A expansão da Internet para além dos computadores e aparelhos celulares, fazendo-se hoje presente em outros sistemas ciberfísicos ou "inteligentes", estende a ameaça de exploração remota para diversas novas tecnologias. Os sistemas e tecnologias atualmente essenciais em nosso cotidiano, como redes de energia, sistemas de controle do tráfego aéreo, satélites, tecnologias médicas, instalações industriais e semáforos, estão conectados à Internet e, portanto, sujeitos a possíveis interferências.

2.5. A Estratégia Nacional de Segurança (NSS) de 2015 reafirmou a ameaça cibernética como sendo um risco de 1° Nível aos interesses do Reino Unido. A NSS expressa a determinação do governo britânico em enfrentar as ameaças cibernéticas e "adotar medidas rigorosas e inovadoras, próprias de um líder mundial em segurança cibernética". Esta Estratégia Nacional de Segurança vem cumprir esse compromisso.

2.6. Na elaboração desta nova estratégia, o governo teve como base as realizações, objetivos e premissas da primeira estratégia nacional quinquenal de segurança cibernética, lançada em 2011. O governo investiu £ 860 milhões ao longo desse período, e temos orgulho do que foi alcançado. As políticas, instituições e ações desenvolvidas nos últimos cinco anos contribuíram para consolidar o Reino Unido como um dos principais atores mundiais em segurança cibernética.

2.7. São bases sólidas já estabelecidas. Entretanto, a persistência e criatividade daqueles que tentam nos ameaçar, a extensão das vulnerabilidades e as deficiências em nossas estruturas e defesas obrigam novos avanços para acompanhar a evolução das ameaças. Será necessária uma abordagem holística se quisermos garantir efetivamente nossos interesses cibernéticos. Nossa determinação em ampliar os investimentos e intervenções tem por base as seguintes premissas:

- a dimensão e a natureza dinâmica das ameaças cibernéticas, bem como a nossa vulnerabilidade e dependência, implicam que a manutenção do modelo existente não será, por si só, suficiente para preservar a nossa segurança;
- a abordagem de confiar ao mercado a tarefa de promover a higiene cibernética não produziu transformações com a agilidade e na escala necessárias. Assim, cabe ao governo exercer liderança nesse sentido e intervir mais diretamente, trazendo sua influência e recursos para enfrentar as ameaças cibernéticas;
- o governo não poderá, isoladamente, contemplar todos os aspectos da segurança cibernética da nação. É necessária uma abordagem integrada e sustentável, em que a população, o setor privado e outros parceiros da sociedade e da administração pública cumpram plenamente suas respectivas funções no processo de garantir a segurança de nossas redes, serviços e dados;
- o Reino Unido necessita de um setor de segurança cibernética pujante e de uma mão

de obra que possa acompanhar, e se antecipar, à evolução das ameaças.

ESCOPO DA ESTRATÉGIA

2.8. Esta estratégia visa, de um lado, orientar as políticas do governo e, do outro, oferecer uma visão coerente e persuasiva aos setores público e privado, à sociedade civil, ao meio acadêmico e à população em geral.

2.9. A estratégia abrange todo o Reino Unido. O governo do Reino Unido atuará na aplicação da estratégia em todos os territórios do Reino Unido e, no que tanger aos assuntos descentralizados, trabalharemos em estreita articulação com os governos regionais em sua aplicação na Escócia, País de Gales e Irlanda do Norte (respeitando as três jurisdições legais separadas e os quatro sistemas educacionais existentes no Reino Unido). No caso de as propostas apresentadas na estratégia se referirem a assuntos de competência regional, a sua implementação será acordada, conforme for o caso, com os referidos governos em conformidade com os respectivos acordos de delegação de competências.

2.10. Esta estratégia define ações propostas ou recomendadas para todos os setores da economia e da sociedade, desde os órgãos do governo central até empresários do setor privado e a população. A estratégia visa fortalecer a segurança cibernética em todos os níveis para o bem coletivo, servindo de base para a atuação internacional do país na promoção da boa governança da Internet.

2.11. Nesta estratégia, entende-se por "segurança cibernética" a proteção aos sistemas de informação (*hardwares*, *softwares* e infraestruturas associadas), aos dados neles contidos e aos serviços que disponibilizam, contra o acesso não autorizado, prejuízos ou uso indevido. Isso inclui prejuízos causados pelo operador do sistema, seja intencionalmente ou acidentalmente ao não seguir os procedimentos de segurança.

2.12. Em consonância com a nossa avaliação dos desafios enfrentados, e tendo como ponto de partida os resultados alcançados no âmbito da estratégia de 2011, este documento estabelece:

- o nosso diagnóstico atualizado do contexto estratégico, incluindo as ameaças atuais e emergentes: quem representa a ameaça mais grave aos nossos interesses e os recursos à sua disposição;
- uma análise das vulnerabilidades e sua evolução nos últimos cinco anos;
- a visão do governo para a segurança cibernética em 2021 e as premissas-chave para alcançar essa meta, incluindo princípios orientadores, atribuições e responsabilidades, e como e onde a intervenção do governo fará a diferença;
- como pretendemos colocar a nossa política em prática: definição das áreas em que o governo exercerá liderança e aquelas em que esperamos atuar em parceria com terceiros; e
- como pretendemos avaliar o progresso face aos objetivos estabelecidos.

3. CONTEXTO ESTRATÉGICO

3.1. À época da publicação da última Estratégia Nacional de Segurança Cibernética, em 2011, a dimensão das transformações tecnológicas e seus impactos já eram aparentes. As tendências e oportunidades nela descritas têm evoluído em ritmo acelerado desde então. Surgiram novas tecnologias e aplicações, e a popularização das tecnologias baseadas na Internet em todo o mundo, e sobretudo nos países em desenvolvimento, ofereceu novas oportunidades de desenvolvimento econômico e social. Essas transformações trouxeram ou trarão vantagens significativas para as sociedades conectadas, como a nossa. Contudo, à medida que cresce a dependência de redes no Reino Unido e no exterior, aumentam também as oportunidades para quem busca comprometer nossos sistemas e dados. Paralelamente, a conjuntura geopolítica mudou. As atividades cibernéticas maliciosas ignoram fronteiras internacionais. Atores estatais passaram a fazer experimentos com recursos cibernéticos ofensivos. Os criminosos cibernéticos têm intensificado suas ações e ampliado seu *modus operandi* estratégico para extrair valores mais elevados de cidadãos, organizações e instituições do Reino Unido. Terroristas e seus simpatizantes vêm promovendo ataques de baixo nível e ambicionam promover atos de maior impacto. Este capítulo descreve o nosso diagnóstico da natureza dessas ameaças, nossas vulnerabilidades e sua constante evolução.

AMEAÇAS

Cibercriminosos

3.2. Esta estratégia trata da cibercriminalidade no contexto de duas formas interrelacionadas de atividade criminosa:

- crimes ciberdependentes – são aqueles que somente podem ser cometidos com recurso às Tecnologias da Informação e Comunicação (TIC), sendo estas ao mesmo tempo o instrumento e o alvo do crime (por exemplo, desenvolvimento e propagação de *malwares* para obtenção de ganhos financeiros, a prática de *hacking* com o objetivo de roubar, danificar, corromper ou destruir dados e/ou redes ou atividades); e
- crimes“ciberfacilitados” (*cyber-enabled*) – crimes tradicionais que podem ter sua escala ou alcance aumentados pelo uso de computadores, redes de computadores ou outras formas de TIC (como fraude e furto de dados).

3.3. Os crimes cibernéticos mais graves praticados contra o Reino Unido, principalmente fraude, furto e extorsão, continuam a ser praticados predominantemente por grupos criminosos organizados de língua russa na Europa Oriental, estando muitos dos serviços do mercado do crime cibernético hospedados nesses países. No entanto, a ameaça também emana de outros países e regiões, e de dentro do próprio Reino Unido, sendo cada vez mais preocupante o surgimento de ameaças no Sul da Ásia e África Ocidental.

3.4. Mesmo quando são identificados os responsáveis pelas atividades cibercriminosas mais prejudiciais ao Reino Unido, muitas vezes o país e as agências policiais internacionais encontram dificuldade em levá-los à justiça quando se encontram em países sem acordos de extradição ou com acordos limitados.

3.5. Esses grupos criminosos são os principais responsáveis pelo desenvolvimento e propagação dos *malwares* cada vez mais avançados que infectam os computadores e redes dos cidadãos do Reino Unido, de suas indústrias e de seu governo. Ainda que o impacto seja pulverizado por todo o país, o efeito cumulativo é significativo. Os ataques vêm se tornando cada vez mais agressivos, fato ilustrado pelo uso crescente de *ransomwares* e ataques de DDoS para fins de extorsão.

3.6. Ainda que grupos criminosos organizados possam representar uma ameaça significativa à nossa prosperidade e segurança coletivas, igualmente preocupante é a ameaça contínua de atos cibernéticos menos sofisticados, porém mais difundidos, praticados contra indivíduos ou organizações de menor porte.

A prática de fraude bancária pela Internet, que inclui saques fraudulentos da conta bancária de um cliente pelo canal de *internet banking*, registrou aumentou de 64% para £ 133,5 milhões em 2015. O aumento menos acentuado no número de casos, de 23%, é evidência, segundo a Financial Fraud Action UK, da tendência de escolher como alvos empresas e clientes com alto poder aquisitivo.

Estados e ameaças patrocinadas por Estados

3.7. São frequentes as tentativas de Estados e grupos patrocinados por Estados de penetrar nas redes do Reino Unido a fim de obter vantagens políticas, diplomáticas, tecnológicas, comerciais e estratégicas, tendo como principal foco os setores de administração pública, defesa, finanças, energia e telecomunicações.

3.8. A capacidade e o impacto desses programas cibernéticos são variados. Os países mais avançados continuam a ampliar suas capacidades em ritmo acelerado, integrando serviços de criptografia e anonimização entre seus recursos, a fim de permanecerem encobertos. Embora tenham a capacidade técnica de lançar ataques sofisticados, muitas vezes é possível atingirem seus objetivos com o uso de recursos e técnicas básicas contra alvos vulneráveis, uma vez que as defesas de suas vítimas são fracas.

3.9. Poucos Estados detêm capacidade técnica para representar uma séria ameaça à segurança e prosperidade geral do Reino Unido. No entanto, são muitos os Estados que vêm desenvolvendo programas cibernéticos sofisticados capazes de representar uma ameaça aos interesses do Reino Unido no futuro próximo. Muitos Estados interessados em desenvolver a capacidade de espionagem cibernética podem adquirir ferramentas prontas voltadas à exploração de redes de computadores, para então adequá-las à espionagem.

3.10. Além da ameaça de espionagem, um pequeno número de atores estrangeiros hostis já desenvolveu e fez uso da capacidade cibernética ofensiva, incluindo a destrutiva. Essa capacidade ameaça a segurança das infraestruturas críticas e sistemas de controle industrial do Reino Unido. Alguns Estados podem utilizar essa capacidade em violação do direito internacional, acreditando poder agir com relativa impunidade, e encorajando outros Estados a seguirem seu exemplo. Embora ainda sejam raros os ataques destrutivos no mundo, continuam a aumentar em número e impacto.

Terroristas

3.11. Grupos terroristas ambicionam promover atividades cibernéticas prejudiciais ao Reino Unido e seus interesses, embora sua capacidade técnica seja atualmente considerada baixa. Todavia, o impacto dessas atividades de baixo nível técnico contra o Reino Unido tem sido desproporcionalmente elevado: ataques simples de *defacement* e *doxing* (prática que consiste em "vazar" na Internet informações acessadas por *hacking*) permitem aos grupos terroristas e seus apoiadores chamar a atenção da imprensa e intimidar suas vítimas.

"O uso que terroristas fazem da Internet para seus propósitos não equivale a ciberterrorismo. No entanto, ao se fazerem cada vez mais presentes no ciberespaço, e dada a disponibilidade do crime cibernético na modalidade de serviço, é possível supor que estariam em condições de lançar ataques cibernéticos"

ENISA Threat Landscape 2015

3.12. A avaliação atual é de que ataques terroristas físicos, e não cibernéticos, continuarão a ser priorizados pelos grupos terroristas no futuro imediato. À medida que uma geração cada vez mais informatizada se envolve com o extremismo, podendo dividir conhecimentos técnicos aprimorados, é possível prever uma escalada de atividades disruptivas de baixa sofisticação (*defacement* ou DDoS) contra o Reino Unido. Também aumentará a probabilidade de surgirem atores extremistas solitários e habilidosos, assim como o risco de que organizações terroristas procurem atrair pessoas do meio para o terrorismo. É provável que os

grupos terroristas utilizem a capacidade cibernética que lhes esteja a dispor para conseguir o máximo efeito possível. Assim, até mesmo um aumento moderado de sua capacidade pode constituir uma ameaça significativa ao Reino Unido e aos seus interesses.

Hacktivistas

3.13. Os hacktivistas são grupos descentralizados e preocupados com as questões da atualidade. Formam e selecionam seus alvos em resposta ao que entendem ser injustiças, introduzindo o caráter de justiceirismo em muitos de seus atos. Enquanto a maioria das atividades cibernéticas dos hacktivistas caracterizam-se pela perturbação (*defacement* de sites ou DDoS), os hacktivistas mais habilidosos têm sido capazes de causar prejuízos maiores e mais duradouros às suas vítimas.

FUNCIONÁRIOS INTERNOS

A ameaça representada por funcionários internos (*insiders*) continua a representar um risco cibernético para as organizações no Reino Unido. Os *insiders* maliciosos, ou seja, funcionários de confiança de uma organização e que têm acesso aos seus sistemas e dados críticos, representam a maior ameaça. Podem causar prejuízos financeiros e à imagem através do furto de dados sigilosos e de propriedade intelectual. Também podem representar uma ameaça cibernética destrutiva se fizerem uso do acesso a informações em virtude de seu cargo para facilitar ou lançar um ataque que interrompa ou degrade serviços críticos na rede de suas organizações, ou para apagar os dados da rede.

Igualmente preocupantes são os *insiders* que, acidentalmente, causam prejuízos cibernéticos ao clicar sem querer em e-mails de *phishing*, conectar *pen-drives* infectados aos computadores ou ignorar os procedimentos de segurança, baixando conteúdos inseguros da Internet. Embora não tenham intenção de prejudicar a organização, seu acesso privilegiado a sistemas e dados implica que suas ações podem causar tantos prejuízos quanto os causados por um *insider* malicioso. Esses indivíduos muitas vezes se tornam vítimas de engenharia social, podendo, desavisadamente, conceder acesso às redes de sua organização ou seguir instruções em boa-fé, beneficiando o criminoso fraudador.

O risco cibernético geral para uma organização proveniente de ameaças internas não se limita ao acesso não autorizado a sistemas de informação e seus conteúdos. São igualmente importantes os controles de segurança física que protegem esses sistemas contra o acesso indevido ou contra o extravio de dados sigilosos ou informações proprietárias em diferentes tipos de mídias. Da mesma forma, uma sólida cultura de segurança, atenta à ameaça representada por funcionários descontentes, por fraude no ambiente de trabalho e por espionagem industrial e outras formas de espionagem, é um elemento fundamental para uma abordagem holística da segurança.

"*Script Kiddies*"

3.14. Os chamados "*script kiddies*", ou seja, indivíduos geralmente menos habilidosos que utilizam *scripts* ou programas desenvolvidos por terceiros para realizar ataques cibernéticos, não são avaliados como uma ameaça significativa à economia ou sociedade em geral. No entanto, esses indivíduos têm acesso a guias, recursos e ferramentas de *hacking* pela Internet. Em razão das vulnerabilidades encontradas nos sistemas expostos à Internet utilizados por muitas organizações, as ações de *script kiddies* podem, em alguns casos, produzir um impacto desproporcionalmente prejudicial na organização atingida.

ESTUDO DE CASO 1: INVASÃO À TALKTALK

Em 21 de outubro de 2015, a operadora britânica TalkTalk relatou um ataque cibernético bem-sucedido e uma possível quebra do sigilo dos dados de seus clientes. A investigação que se sucedeu apurou que houve acesso a um banco de dados de clientes através de servidores virtuais acessíveis ao público, colocando em risco os dados cadastrais de aproximadamente 157.000 clientes, incluindo seus nomes, endereços e dados bancários.

No mesmo dia, diversos funcionários da TalkTalk receberam um e-mail com pedido de resgate em Bitcoins. Os responsáveis pelo ataque descreveram em detalhe a estrutura do banco de dados como prova de que havia sido acessado.

A comunicação do incidente feita pela TalkTalk ajudou a polícia, com apoio de especialistas da Agência Nacional de Criminologia, a prender os principais suspeitos, todos localizados no Reino Unido, em outubro e novembro de 2015.

O ataque demonstra que, mesmo em grandes organizações com elevado nível de conhecimento cibernético, as vulnerabilidades podem persistir. A exploração dessas vulnerabilidades pode causar efeito desproporcional em termos de danos à imagem e transtornos operacionais, tendo este incidente gerado grande repercussão na imprensa. A rápida comunicação do ocorrido por parte da TalkTalk permitiu que a polícia agisse com agilidade, e possibilitou tanto à população quanto ao governo mitigar a possível perda de dados sigilosos. O incidente custou à TalkTalk cerca de £ 60 milhões e a perda de 95.000 clientes, além de uma desvalorização acentuada de suas ações no mercado.

ESTUDO DE CASO 2: ATAQUE AO SISTEMA SWIFT DO BANCO DE BANGLADESH

A Sociedade de Telecomunicações Financeiras Interbancárias Mundiais (*Society for Worldwide Interbank Financial Telecommunication – SWIFT*) disponibiliza uma rede que permite que instituições financeiras em todo o mundo enviem e recebam informações sobre transações financeiras com garantia de segurança. Uma vez que a rede SWIFT envia ordens de pagamento que devem ser liquidadas por contas correspondentes mantidas entre as instituições, existe há muito tempo uma preocupação sobre a possibilidade de esse processo ser comprometido por cibercriminosos ou outros atores maliciosos que tentem injetar ordens de pagamento ilegítimas ou, na pior das hipóteses, tentem incapacitar ou interromper o funcionamento da própria rede SWIFT.

No início de fevereiro de 2016, um criminoso cibernético acessou o sistema de pagamentos SWIFT do Banco de Bangladesh e instruiu o Federal Reserve de Nova York a transferir dinheiro da conta mantida pelo Banco do Bangladesh para contas nas Filipinas. A tentativa de fraude envolveu o montante de US$ 951 milhões. O sistema bancário impediu a realização de 30 operações, no valor total de US$ 850 milhões. No entanto, cinco transações, totalizando US$ 101 milhões, conseguiram passar. Destes, foram recuperados US$ 20 milhões no Sri Lanka. Os US$ 81 milhões restantes, transferidos para as Filipinas, passaram por lavagem em casinos e parte dos recursos foi enviada a Hong Kong.

A investigação forense promovida pelo Banco de Bangladesh apurou que havia sido instalado um *malware* nos sistemas do banco e este havia sido usado para coletar informações sobre os procedimentos usados pelo banco em pagamentos e transferências internacionais. Uma análise mais aprofundada feita pela BAE Systems no *malware* ligado ao ataque revelou sofisticados recursos de interação com a instância local de um *software* denominado Alliance Access, ligado ao sistema SWIFT, que rodava na infraestrutura do Banco de Bangladesh. A BAE concluiu que "os criminosos vêm promovendo ataques cada vez mais sofisticados contra as organizações vítimas, sobretudo na área de intrusões de rede".

ESTUDO DE CASO 3: ATAQUE ÀS REDES DE ENERGIA DA UCRÂNIA

Em 23 de dezembro de 2015, um ataque cibernético contra as distribuidoras ucranianas Prykarpattya Oblenergo e Kyiv Oblenergo causou um grande apagão ao interromper o funcionamento de mais de 50 subestações nas redes de distribuição. A região teria sofrido uma interrupção no abastecimento de energia por várias horas, enquanto outros clientes e áreas sofreram interrupções de menor duração, sendo afetados mais de 220.000 consumidores no total.

O uso do *malware* BlackEnergy3 foi atribuído por alguns ao ataque, após serem identificas amostras do *software* malicioso na rede. Pelo menos seis meses antes do ataque, os *hackers* responsáveis enviaram e-mails de *phishing* aos escritórios das concessionárias de energia elétrica

na Ucrânia, contendo documentos maliciosos em Microsoft Office. No entanto, é improvável que o *malware* tenha sido responsável pela abertura dos disjuntores que resultou na interrupção. É mais provável que o *malware* tenha servido para coletar dados de login, e que estes tenham, então, possibilitado assumir o controle remoto direto de determinados aspectos da rede, permitindo derrubar a rede elétrica.

O incidente na Ucrânia é o primeiro caso confirmado de um ataque cibernético que tenha interrompido o funcionamento de uma rede de energia. Casos como esse demonstram ainda a necessidade de aplicar boas práticas de segurança cibernética em toda as infraestruturas críticas nacionais para evitar a ocorrência de incidentes similares no Reino Unido.

VULNERABILIDADES

Um leque cada vez mais variado de dispositivos conectados

3.15. Quando da publicação da última Estratégia Nacional de Segurança Cibernética, em 2011, a maioria das pessoas associava a segurança cibernética à proteção de dispositivos como computadores *desktop* ou *notebook*. Desde então, a Internet passou a integrar cada vez mais o nosso cotidiano através de novas formas conectividade, em grande parte desconhecidas. A "Internet das Coisas" cria novas oportunidades de exploração e aumenta o impacto potencial de ataques capazes de provocar danos físicos, lesões pessoais e, na pior das hipóteses, morte.

3.16. A rápida expansão da conectividade nos processos de controle industrial de sistemas críticos nos mais diversos setores, como energia, mineração, agricultura e aviação, criou a chamada Internet das Coisas Industrial. Esse fenômeno simultaneamente cria a possibilidade de ocorrer invasão e adulteração de dispositivos e processos nunca antes vulneráveis a tal interferência, com consequências possivelmente desastrosas.

3.17. Portanto, não somos mais vulneráveis apenas aos danos virtuais causados pela falta de segurança cibernética em nossos próprios dispositivos; estão sob ameaça os sistemas interligados que são fundamentais à nossa sociedade, saúde e bem-estar.

Falta de higiene cibernética e cumprimento de normas

3.18. A conscientização britânica das vulnerabilidades técnicas em *softwares* e redes e da necessidade de higiene cibernético tem, sem dúvida, crescido ao longo dos últimos cinco anos. Isso se deve, em parte, a iniciativas do governo como os "10 Passos para a Segurança Cibernética", mas também à maior visibilidade e impacto dos incidentes cibernéticos envolvendo governos e corporações. Os ataques cibernéticos não são necessariamente sofisticados ou inevitáveis, sendo frequentemente uma consequência da exploração de vulnerabilidades facilmente corrigíveis e, muitas vezes, preveníveis. Na maioria dos casos, ainda é a vulnerabilidade da vítima, e não a engenhosidade do cibercriminoso, o fator decisivo no sucesso de um ataque cibernético. As empresas e as organizações decidem onde e como investir na segurança cibernética a partir de análises de custo-benefício, mas são, em última análise, os responsáveis pela segurança de seus dados e sistemas. Somente combatendo os riscos de ataques cibernéticos aos seus sistemas críticos e dados sigilosos, com investimentos adequados em equipes, tecnologias e governança, é que as empresas serão capazes de reduzir sua exposição a possíveis prejuízos cibernéticos.

"Não existe um sistema de segurança de informações capaz impedir uma única pessoa entre cem de abrir um e-mail de *phishing*, e isso pode bastar para comprometer o sistema".

Ciaran Martin, Diretor-Geral da Cyber Security, GCHQ – Junho de 2015

Falta de capacitação e conhecimentos

3.19. Faltam competências e conhecimentos necessários para atender às necessidades de segurança cibernética nos setores público e

privado. Nas empresas, muitos funcionários não têm conhecimentos em segurança cibernética e não compreendem suas responsabilidades a este respeito, em parte pela falta de capacitação formal. Também falta uma maior conscientização sobre segurança cibernética na população em geral.

"Pouco menos de um quinto das empresas promoveu capacitações de segurança cibernética para seus colaboradores no ano passado."
Cyber Security Breaches Survey 2016.

3.20. Também precisamos desenvolver conhecimentos e competências especializadas que permitam acompanhar a rápida evolução da tecnologia e controlar os riscos cibernéticos associados. Esse déficit de competências representa uma vulnerabilidade nacional que deve ser sanada.

Sistemas legados sem *patch* de correção

3.21. Muitas organizações localizadas no Reino Unido continuarão a usar sistemas legados vulneráveis até o próximo processo de modernização de TI. Os *softwares* nesses sistemas muitas vezes utilizam versões mais antigas e sem *patch* de correção. Essas versões mais antigas frequentemente apresentam vulnerabilidades que cibercriminosos procuram por possuírem ferramentas capazes de explorá-las. Outro problema é o uso por parte de algumas organizações de *softwares* não suportados, para os quais não existem *patches* publicados.

"Recentemente, analisamos 115.000 dispositivos Cisco na Internet e nos ambientes de clientes como uma forma de chamar a atenção para os riscos de segurança da infraestrutura envelhecida atual e da falta de atenção com as correções de falhas de vulnerabilidades... Descobrimos que 106.000 dos 115.000 dispositivos apresentavam vulnerabilidades conhecidas no *software* que executavam."
Cisco 2016 Annual Security Report

Disponibilidade de recursos de *hacking*

3.22. A pronta disponibilidade na Internet de informações sobre *hacking* e de ferramentas de *hacking* fáceis de usar permite aos interessados desenvolver a capacidade de exercer a prática. As informações necessárias aos *hackers* para comprometer a segurança das vítimas muitas vezes são facilmente acessíveis e podem ser colhidas com rapidez. Todos, seja em casa ou no ambiente corporativo, devem estar conscientes do grau de exposição de seus dados pessoais e sistemas na Internet, e de quanto essa exposição pode deixá-los vulneráveis à exploração cibernética maliciosa.

"99,9% das vulnerabilidades exploradas ocorreram mais de um ano após a divulgação da vulnerabilidade."
Relatório de Investigações da Verizon sobre a Violação de Dados em 2015

CONCLUSÕES

3.23. O Reino Unido criou políticas e instituições que fortaleceram suas defesas e tiveram êxito em mitigar algumas das ameaças enfrentadas no ciberespaço.

3.24. No entanto, ainda não estamos um passo à frente da ameaça. Embora a natureza e as motivações dos atores cibernéticos maliciosos que temos de combater sejam em grande parte as mesmas, o volume de *malwares* e o número de atores maliciosos cresceu rapidamente. Aumentou-se a capacidade de nossos adversários mais tecnicamente competentes, um número seleto de estados e cibercriminosos de elite. Nosso desafio coletivo consiste em garantir que nossas defesas sejam evoluídas e ágeis o bastante para enfrentá-los, reduzir a capacidade de ataque de atores maliciosos e tratar das causas das vulnerabilidades descritas acima.

4. NOSSA RESPOSTA NACIONAL

4.1. Para mitigar as diversas ameaças que enfrentamos e salvaguardar nossos interesses no ciberespaço, precisamos de uma abordagem estratégica que norteie todas as nossas ações coletivas e individuais no domínio digital durante os próximos cinco anos. Esta seção define nossa visão e abordagem estratégica.

NOSSA VISÃO

4.2. Nossa visão para 2021 é que o Reino Unido seja um país seguro e resiliente às ameaças cibernéticas, próspero e confiante no mundo digital.

4.3. Para concretizar esta visão, teremos como objetivos:

• **DEFENDER** Devemos dispor dos meios para defender o Reino Unido contra a evolução das ameaças cibernéticas, para responder com eficácia à ocorrência de incidentes e para garantir que as redes, dados e sistemas do país sejam seguros e resilientes. A população, as empresas e o setor público devem ter os conhecimentos e a capacidade de se defenderem.

• **DISSUADIR** O Reino Unido não será alvo fácil para qualquer forma de agressão no ciberespaço. Devemos detectar, entender, investigar e frustrar as ações hostis empreendidas contra o país, perseguindo e levando a juízo os infratores. Devemos dispor de meios para promover ações ofensivas no ciberespaço, se assim optarmos.

• **DESENVOLVER** Devemos dispor de uma indústria de segurança cibernética inovadora e em expansão, apoiada por pesquisa e produção científica de ponta. Teremos uma safra de talentos com conhecimentos que atendam às necessidades nacionais nos setores público e privado. Nossas análises e conhecimentos avançados permitirão ao país enfrentar e superar as ameaças e desafios futuros.

4.4. Em busca desses objetivos, empreenderemos **AÇÕES INTERNACIONAIS** e exerceremos a nossa influência através do investimento em parcerias. Conduziremos a evolução global do ciberespaço ao encontro dos nossos interesses econômicos e de segurança.

PRINCÍPIOS

4.5 Em sua busca desses objetivos, o governo terá como diretrizes os seguintes princípios:

- nossas ações e políticas serão motivadas pela necessidade de proteger nosso povo e ampliar a nossa prosperidade;
- qualquer ataque cibernético ao Reino Unido será tratado com a mesma seriedade que um ataque convencional, tomando-se todas as medidas necessárias em nossa defesa;
- agiremos de acordo com a legislação nacional e internacional, e esperamos que terceiros façam o mesmo;
- protegeremos com rigor e promoveremos os nossos valores fundamentais. Dentre eles estão a democracia; o estado de direito; a liberdade; a transparência e a prestação de contas pelos órgãos e instituições públicas; os direitos humanos; e a liberdade de expressão;
- preservaremos e protegeremos a privacidade dos cidadãos britânicos;
- trabalharemos em parceria. A segurança do Reino Unido no ciberespaço depende da articulação com as Administrações Regionais, os diversos atores do setor público, as empresas, as instituições e a população;
- o governo assumirá as suas responsabilidades e coordenará a resposta nacional, mas cabe às empresas, organizações e população tomar as medidas cabíveis para garantir a sua proteção na Internet, bem como sua resiliência e continuidade operacional na ocorrência de um incidente;
- a responsabilidade pela segurança dos órgãos do setor público, inclusive pela sua segurança cibernética e pela proteção dos dados e serviços online, cabe aos respectivos Ministros, Secretários Permanentes e Conselhos de Administração;

- não aceitaremos riscos significativos ao público e ao país como um todo em razão da falta de tomada de medidas por parte de empresas e organizações para controlar as ameaças cibernéticas;
- trabalharemos em estreita colaboração com os países que partilham da nossa visão e cuja segurança se sobreponha com a nossa, reconhecendo que as ameaças cibernéticas ignoram fronteiras. Também teremos uma ampla atuação junto a parceiros internacionais visando influenciar a comunidade global, reconhecendo o valor de grandes coligações; e
- a fim de garantir que as intervenções do governo causem um impacto significativo na segurança e resiliência cibernética do país, procuraremos definir, analisar e apresentar dados diagnósticos do estado da segurança cibernética coletiva e do grau de cumprimento de nossos objetivos estratégicos.

ATRIBUIÇÕES E RESPONSABILIDADES

4.6. A garantia da segurança do ciberespaço nacional exigirá um esforço coletivo. Cada um de nós tem um papel importante a desempenhar.

Indivíduos

4.7. Seja como cidadãos, funcionários ou consumidores, sempre tomamos medidas práticas para garantir a segurança dos bens que valorizamos no mundo físico. No mundo virtual, devemos fazer o mesmo. Devemos cumprir nossa responsabilidade pessoal por tomar todas as medidas cabíveis para proteger não apenas os nossos equipamentos físicos, ou seja, aparelhos de celular e outros dispositivos, mas também os dados, *softwares* e sistemas que nos trazem liberdade, flexibilidade e conveniência em nossas vidas privadas e profissionais.

Empresas e organizações

4.8. As empresas, as organizações dos setores público e privado e outras instituições detêm dados pessoais, prestam serviços e operam sistemas no domínio digital. A conectividade dessas informações revolucionou suas atividades. Entretanto, essa transformação tecnológica veio acompanhada da responsabilidade de proteger os ativos que eles detêm, manter os serviços que prestam e dotar os produtos que comercializam de um nível adequado de segurança. O cidadão e o consumidor, bem como a sociedade em geral, esperam que as empresas e organizações tomem todas as medidas cabíveis para proteger os seus dados pessoais e que a resiliência, ou seja, a capacidade de suportar e se recuperar de incidentes, seja incorporada nos sistemas e estruturas dos quais dependem. As empresas e organizações também devem entender que, caso sejam vítimas de um ataque cibernético, serão responsabilizadas civilmente pelas consequências.

Governo

4.9. O dever primordial do governo consiste em defender o país dos ataques de outros Estados, proteger os cidadãos e a economia contra prejuízos e criar os meios em âmbito nacional e internacional para proteger os nossos interesses, salvaguardar os direitos fundamentais e levar os criminosos à justiça.

4.10. Em sua qualidade de detentor de um volume significativo de dados e prestador de serviços, o governo toma medidas rigorosas para a salvaguarda de seus ativos de informação. Outra atribuição importante do governo é o de orientar e informar a população e as organizações sobre as medidas necessárias para se protegerem na Internet e, quando necessário, definir as normas a serem seguidas por empresas e organizações-chave.

4.11. Embora os setores-chave da economia estejam em mãos privadas, cabe ao governo, em última instância, assegurar a resiliência nacional e, em conjunto com seus parceiros na administração pública, a manutenção dos serviços e funções essenciais de governo.

Promovendo a transformação: o papel do mercado

4.12. A Estratégia de 2011 e o Programa Nacional de Segurança Cibernética procuraram estimular a busca de resultados e o aumento da capacidade cibernética tanto no setor público quanto no privado, recorrendo ao mercado para estimular os comportamentos corretos. Esperava-se que as pressões econômicas e os incentivos promovidos pelo governo seriam capazes de garantir um investimento privado adequado em segurança cibernética, estimular os fluxos de investimento no setor e promover a formação de profissionais qualificados no tema.

4.13. Muito foi alcançado. Nos últimos cinco anos, em toda a economia e na sociedade em geral, houve uma maior conscientização dos riscos e das ações necessárias para mitigar os riscos cibernéticos. Mas a combinação das forças de mercado com incentivos do governo mostrou-se insuficiente, por si só, para assegurar os nossos interesses de longo prazo no ciberespaço com a celeridade necessária. Muitas redes, inclusive em setores críticos, ainda não são seguras. O mercado ainda não valoriza, e portanto não controla, o risco cibernético adequadamente. São muitas as organizações que ainda sofrem com violações até mesmo no nível mais básico. São poucos os investidores dispostos a arriscar-se a apoiar os empresários do setor. São poucos os formandos e outros profissionais com competências adequadas sendo formados pelo sistema de ensino superior.

4.14. O mercado ainda tem um papel a desempenhar e, a longo prazo, produzirá um impacto maior do que o governo jamais conseguiria. No entanto, a urgência da ameaça enfrentada pelo Reino Unido e a expansão das vulnerabilidades do nosso ambiente digitalizado exigem do governo maiores ações no curto prazo.

Promovendo a transformação: um papel mais amplo para o governo

4.15. O governo deve, portanto, ditar o ritmo do processo de atendimento às necessidades nacionais em segurança cibernética. Somente o governo será capaz de fazer uso de seus recursos de inteligência e outros necessários para defender o país das ameaças mais sofisticadas. Somente o governo poderá promover a cooperação entre os setores público e privado e assegurar o intercâmbio de informações entre ambos. O governo assumirá um papel de liderança, sempre em consulta com a iniciativa privada, na definição das boas práticas de segurança cibernética e na sua implementação.

4.16. O governo trará melhorias significativas na segurança cibernética nacional ao longo dos próximos cinco anos. Este programa ambicioso e transformador terá como foco as quatro áreas principais a seguir:

- **Alavancas e incentivos**. O governo investirá para maximizar as potencialidades de um setor cibernético verdadeiramente inovador. Para isso, será dado apoio a *start-ups* e serão feitos investimentos em inovação. Também procuraremos identificar e atrair talentos precocemente no sistema de ensino, além de desenvolver rotas mais claras para uma profissão que precisa de melhor definição. O governo também utilizará todos os meios disponíveis, incluindo o futuro Regulamento Geral da Proteção de Dados (GDPR), para elevar os padrões de segurança cibernética em toda a economia, inclusive, se necessário, através da regulamentação.
- **Maior inteligência e fiscalização com foco na ameaça**. As agências de inteligência, o Ministério da Defesa, a polícia e a Agência Nacional de Criminologia, em articulação com agências internacionais parceiras, redobrarão seus esforços para identificar, antecipar e coibir atividades cibernéticas hostis por parte de atores estrangeiros, cibercriminosos e terroristas. Essa atuação contribuirá para melhorias na aquisição e exploração de inteligência, permitindo obter inteligência preventiva sobre a intenção e a capacidade de nossos adversários.
- **Desenvolvimento e aplicação de tecnologias** em parceria com o setor privado, incluindo medidas de Defesa Cibernética Ativa, a fim de aprofundar a compreensão das ameaças, reforçar a segurança dos sistemas e redes dos setores público e privado no Reino Unido diante dessa ameaça, além de coibir atividades maliciosas.
- **Centro Nacional de Segurança Cibernética (NCSC)**. O governo criou um órgão central para a segurança cibernética a nível nacional. A esse órgão caberá responder a incidentes cibernéticos nacionais, atuar como voz autorizada e centro de

referência em segurança cibernética, bem como prestar serviços customizados de suporte e assessoria a repartições públicas, administrações regionais, reguladores e empresas. O NCSC será responsável por analisar, detectar e entender as ameaças cibernéticas, bem como contribuir com seus conhecimentos em segurança cibernética em apoio aos esforços envidados pelo governo para promover a inovação, fomentar uma indústria de segurança cibernética dinâmica e estimular o desenvolvimento de competências em segurança cibernética. De forma inédita para um órgão público desta natureza, o NCSC está vinculado ao GCHQ e, portanto, possui acesso aos conhecimentos de ponta e capacidades sensíveis dessa organização, valorizando o apoio a ser oferecido à economia e à sociedade em geral. Será responsabilidade de cada departamento do governo aplicar de forma eficaz as orientações recebidas sobre segurança cibernética.

"Tendo em vista o furto em escala industrial da propriedade intelectual de nossas empresas e universidades, bem como os numerosos golpes de *phishing* e *malware*s que geram perdas de tempo e dinheiro, a criação do Centro Nacional de Segurança Cibernética demonstra que o Reino Unido está envidando esforços para combater as ameaças existentes na Internet."

Robert Hannigan, Diretor do GCHQ, março de 2016

4.17. A busca dessa transformação em nossa segurança e resiliência cibernéticas exigirá novos recursos. No documento *Strategic Defence and Security Review 2015*, o Governo destinou £ 1,9 bilhão ao cumprimento desses compromissos e objetivos ao longo do horizonte de cinco anos da estratégia.

CENTRO NACIONAL DE SEGURANÇA CIBERNÉTICA

Inaugurado em 1° de outubro de 2016, o Centro Nacional de Segurança Cibernética (NCSC) representa uma oportunidade única para a construção de parcerias em segurança cibernética entre o governo, a iniciativa privada e a população, contribuindo para o fortalecimento da segurança online no Reino Unido. O Centro será responsável pela resposta a incidentes cibernéticos e servirá como referência em segurança cibernética no país. De forma inédita, haverá uma interação direta entre setores-chave e a equipe do NCSC, permitindo o acesso aos melhores serviços de consultoria e suporte relacionados à proteção de redes e sistemas contra ameaças cibernéticas.

O NCSC atua como:

• fonte centralizada de inteligência e informações sobre ameaças à segurança cibernética para o governo;
• a face ostensiva das ações do governo contra ameaças cibernéticas, trabalhando em parceria com a iniciativa privada, o meio acadêmico e parceiros internacionais para manter o Reino Unido a salvo de ataques cibernéticos; e
• uma organização voltada ao público e articulada com o GCHQ, podendo nele acessar informações de inteligência necessariamente sigilosas e os conhecimentos técnicos mais avançados.

A construção da estrutura do NCSC será conduzida em etapas ao longo do horizonte desta estratégia. O centro reúne as estruturas já desenvolvidas pela CESG, braço de segurança da informação do GCHQ: o Centro para a Proteção das Infraestruturas Nacionais (CPNI), a CERT-UK (*Computer Emergency Response Team*) e o Centro de Análise Cibernética (CCA). Desta forma, serão aproveitados os melhores recursos já implantados, ao mesmo tempo em que as estruturas anteriores serão simplificadas. O Centro terá como objetivos iniciais:

• oferecer uma estrutura de resposta a incidentes de classe mundial, destinado a tratar e reduzir os prejuízos causados por incidentes cibernéticos, desde aqueles que afetam organizações isoladas até os ataques nacionais em grande escala;
• divulgar informações sobre as atitudes que podem ser adotadas por organizações do setor público e privado para lidar com questões de segurança cibernética, facilitando o intercâmbio de informações sobre ameaças cibernéticas; e
• prestar consultoria setorial especializada ao governo e a setores críticos, como os de telecomunicações, energia e finanças, assim como orientações e diretrizes de segurança cibernética aplicáveis em geral.

O NCSC oferece os meios para viabilizar muitos dos elementos desta estratégia. Reconhecemos que, com o desenvolvimento do NCSC, seu foco e suas estruturas terão de se adaptar aos novos desafios e aos aprendizados acumulados.

PLANO DE IMPLEMENTAÇÃO

Nossos objetivos para a segurança cibernética do país nos próximos cinco anos são naturalmente ambiciosos. Para alcançá-los, será preciso agir com seriedade e determinação em todo ambiente digital. As ações para a concretização da visão do governo se darão nos três principais eixos da estratégia: DEFENDER nosso ciberespaço, DISSUADIR nossos adversários e DESENVOLVER a nossa capacidade, todos respaldados por uma AÇÃO INTERNACIONAL eficaz.

5. DEFENDER

5.0.1. Os elementos do eixo DEFENDER visam assegurar que as redes, dados e sistemas do Reino Unido, nas esferas pública, econômica e privada, sejam resilientes e protegidos contra ataques cibernéticos. Jamais será possível deter todos os ataques cibernéticos, assim como não é possível deter todos os crimes. No entanto, trabalhando em conjunto com a população, instituições de ensino, universidades, empresas e outros governos, podemos construir camadas de defesa capazes de reduzir de forma significativa a nossa exposição a incidentes cibernéticos, proteger os nossos bens mais preciosos e permitir que todos convivam e prosperem no ciberespaço. A promoção da cooperação entre Estados e das boas práticas de segurança cibernética também é do interesse da nossa segurança coletiva.

5.0.2. O governo adotará medidas para garantir que cidadãos, empresas, organizações e instituições públicas e privadas tenham acesso às informações necessárias para se defenderem. O Centro Nacional de Segurança Cibernética atua como fonte unificada de inteligência e informações sobre ameaças à segurança cibernética, permitindo oferecer consultoria individualizada sobre defesa cibernética e responder com agilidade e eficácia a incidentes de grande dimensão no espaço cibernético. O governo trabalhará em parceria com a iniciativa privada e com parceiros internacionais na definição de boas práticas de segurança cibernética para os setores público e privado, para os nossos sistemas e serviços mais essenciais e para a economia em geral. A segurança será incorporada na concepção de todos os novos sistemas da administração pública e sistemas críticos. As agências policiais devem manter estreita colaboração com a iniciativa privada e com o Centro Nacional de Segurança Cibernética, fornecendo informações dinâmicas de inteligência sobre ameaças criminais que permitam ao setor privado defender-se da melhor maneira, e emitindo orientações e padrões de segurança para sua proteção.

5.1. DEFESA CIBERNÉTICA ATIVA

5.1.1. A Defesa Cibernética Ativa (*Active Cyber Defense – ACD*) consiste em adotar medidas de segurança capazes de fortalecer uma rede ou sistema e torná-lo mais robusto contra ataques. Em um contexto não governamental, a Defesa Cibernética Ativa geralmente se refere à atuação de analistas de segurança cibernética no diagnóstico das ameaças às suas redes e na formulação e implementação de medidas proativas de combate ou defesa contra essas ameaças. No contexto desta estratégia, o governo optou por aplicar o mesmo princípio numa escala maior: utilizará seus conhecimentos, estruturas e influência para revolucionar a segurança cibernética nacional face às ameaças cibernéticas. A "rede" a ser defendida, neste caso, é todo o espaço cibernético nacional. As atividades propostas representam um plano de ação defensivo, baseando-se na experiência do NCSC como autoridade técnica nacional para responder a ameaças cibernéticas ao Reino Unido a um nível macro.

Objetivos

5.1.2. Nas ações de Defesa Cibernética Ativa, o governo terá como objetivo:

- tornar o Reino Unido um alvo muito mais difícil de ser atingido por atores patrocinados por Estados e cibercriminosos, aumentando a resiliência das redes do país;
- derrotar a vasta maioria dos malwares de alto volume/baixa sofisticação nas redes do Reino Unido, bloqueando a comunicação promovida pelos malwares entre os hackers e suas vítimas;
- aprimorar e aumentar o alcance e a escala das estruturas do governo destinados a deter ameaças criminosas graves patrocinadas por Estados ou promovidos por cibercriminosos;
- proteger o tráfego na Internet e de telefonia contra a tomada de controle por atores maliciosos;
- robustecer as infraestruturas críticas e os serviços ao cidadão contra ameaças cibernéticas; e
- frustrar o modelo de negócios de cibercriminosos de todos os tipos,

desmotivando-os e reduzindo os prejuízos provocados por seus ataques.

Abordagem

5.1.3. Na busca por tais objetivos, o governo pretende:

- trabalhar em parceria com a iniciativa privada, sobretudo as operadoras de telecomunicações, para dificultar significativamente o ataque a serviços e usuários de Internet no Reino Unido e reduzir de forma expressiva a possibilidade de haver impactos prolongados em função de ataques no Reino Unido. Essa atuação deve incluir esforços de combate às práticas de phishing, o bloqueio de domínios e endereços IP maliciosos, além de outras medidas para deter os ataques com malwares. Incluirá também medidas para proteger as infraestruturas de telecomunicações e de encaminhamento do Reino Unido;
- ampliar a escala e a capacidade do GCHQ, do Ministério da Defesa e da Agência Nacional de Criminologia para deter ameaças cibernéticas mais graves ao Reino Unido, incluindo campanhas promovidas por cibercriminosos sofisticados e atores estrangeiros hostis; e
- proteger com maior eficácia os sistemas e redes governamentais, ajudar o setor privado a reforçar a segurança da cadeia de fornecimento das infraestruturas críticas, tornar o ecossistema de softwares mais seguro e implantar proteções automatizadas nos serviços públicos virtuais disponibilizados ao cidadão.

5.1.4. Sempre que possível, essas iniciativas serão realizadas conjuntamente ou por meio de parcerias com a iniciativa privada. Em muitos casos, a concepção e implementação caberiam à iniciativa privada, competindo ao governo os processos fundamentais de apoio, assessoria e orientação conceitual.

5.1.5. O governo também realizará ações específicas para a implementação dessas medidas, dentre elas:

- atuação conjunta com empresas de telecomunicações no bloqueio de ataques de *malware*. Essa atuação se dará pela restrição do acesso a domínios ou sites específicos de origem de *malwares*. Essa técnica é conhecida como bloqueio/filtragem de DNS (Domain Name System);
- combate a atividades de *phishing* com uso de "*spoofing*" de domínio (envio de e-mails que parecem ser de determinado remetente oficial, como um banco ou órgão público, mas que na realidade são golpes) com a implantação de um sistema-padrão de verificação de e-mails nas redes governamentais, e incentivo à prática no setor privado;
- promoção das melhores práticas de segurança através de organizações multi-participadas de governança da Internet, como a Internet Corporation for Assigned Names and Numbers (ICANN), que coordena o Domain Name System (DNS), a Internet Engineering Task Force (IETF) e o European Internet Regional Registry (RIPE), bem como diálogo com partes interessadas no Fórum de Governança da Internet (IGF) das Nações Unidas;
- atuação junto aos órgãos policiais no sentido de proteger os cidadãos britânicos de ataques cibernéticos promovidos a partir de infraestruturas desprotegidas no exterior;
- implementação de controles para garantir a segurança do tráfego de Internet para os órgãos públicos, impedindo seu reencaminhamento ilícito por atores maliciosos; e
- investimento em programas do Ministério da Defesa, da NCA e do GCHQ para fortalecer a capacidade dessas organizações de responder e desarticular as atividades cibernéticas de elevada gravidade praticadas por criminosos e patrocinadas por Estados e que tenham como alvo as redes britânicas.

O desenvolvimento dessas intervenções técnicas deve acompanhar a evolução das ameaças, garantindo que a população e as empresas do Reino Unido estejam sempre protegidas contra a maioria dos ataques cibernéticos em larga escala.

Avaliação dos resultados

5.1.6. O êxito do governo em estabelecer um programa eficaz de Defesa Cibernética Ativa será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- dificultação de ações de "*phishing*" por meio de defesas em grande escala contra a utilização de domínios maliciosos e uma proteção *antiphishing* mais ativa, e dificultação do uso de outras formas de comunicação, como "*vishing*" e *spoofing* de SMS, em ataques de engenharia social;
- bloqueio de uma proporção muito maior das comunicações de *malwares* e artefatos técnicos associados a ataques e exploração cibernética;
- o tráfego de Internet e de telecomunicações no Reino Unido apresentar uma vulnerabilidade significativamente menor a reencaminhamento por atores maliciosos;
- fortalecimento expressivo da capacidade de resposta do GCHQ, das Forças Armadas e da NCA diante de graves ameaças patrocinadas por Estados e criminosos.

5.2. CONSTRUÇÃO DE UMA INTERNET MAIS SEGURA

5.2.1. A evolução tecnológica traz oportunidades para reduzir significativamente a capacidade de nossos adversários de promover crimes cibernéticos no Reino Unido por meio de esforços para garantir que os produtos e serviços online comercializados no futuro tenham a segurança integrada por padrão. Nesse sentido, os controles de segurança incorporados nos *softwares* e nos *hardwares* que utilizamos devem ser ativados de fábrica como configuração padrão, para que o usuário possa contar com a segurança máxima oferecida a menos que opte por desativá-la. O desafio consiste em promover essa transformação de uma forma que atenda ao usuário final e ofereça um produto ou serviço comercialmente viável, porém seguro – tudo dentro da premissa de manter a natureza livre e aberta da Internet.

"A variedade de dispositivos conectados à Internet se multiplica rapidamente. Foram registrados diversos ataques ainda na fase de prova de conceito, assim como no ambiente de produção em 2015, sendo verificadas vulnerabilidades graves em carros, dispositivos médicos, entre diversos outros. Os fabricantes devem priorizar a segurança para reduzir o risco de graves consequências pessoais, econômicas e sociais".

Symantec, Relatório de Ameaças à Segurança na Internet 2016

5.2.2. O governo está bem posicionado para assumir um papel de liderança no uso dessas novas tecnologias para fortalecer a proteção de sistemas próprios, contribuir para a construção da segurança na cadeia de suprimentos do setor privado, proteger o ecossistema de *softwares* e fornecer proteções automatizadas aos cidadãos que acessem os serviços públicos online. O governo deve testar e implementar novas tecnologias que integrem proteções automatizadas nos produtos e serviços públicos online. Sempre que possível, devem ser oferecidas tecnologias similares ao setor privado e à população.

Objetivo

5.2.3. Até 2021, a maioria dos novos lançamentos de produtos e serviços online deve ter a segurança integrada por padrão. Os consumidores devem ter à sua escolha produtos e serviços que tenham a segurança incorporada como configuração padrão. O usuário poderá desativar essas configurações se assim preferir, mas quem desejar interagir com o ciberespaço da maneira mais segura deve sempre estar automaticamente protegido.

Nossa abordagem

5.2.4. Serão adotadas as seguintes ações:

- O Governo dará o exemplo, disponibilizando serviços eletrônicos seguros que não dependam da segurança da própria Internet;
- Serão exploradas alternativas de parceria com o setor privado para o desenvolvimento de tecnologias de ponta capazes de integrar uma maior segurança "por padrão" nos hardwares e softwares; e

- Serão adotadas novas tecnologias de segurança cibernética no governo, estimulando as administrações regionais a fazer o mesmo, a fim de reduzir os riscos percebidos de sua adoção. Tal adoção servirá como prova de conceito, demonstrando os benefícios à segurança das novas tecnologias e técnicas. Também contribuirá para inserir a segurança como elemento central no desenvolvimento de novos produtos, eliminando oportunidades para a exploração criminosa e protegendo, desta forma, o usuário final.

5.2.5. Para isso, pretende-se:

- continuar a incentivar os fornecedores de *hardwares* e *softwares* a comercializar produtos com configurações de segurança ativadas por padrão, exigindo que o usuário desabilite deliberadamente essas configurações para torná-las inseguras. Alguns fornecedores já adotaram essa prática, enquanto outros ainda não tomaram as medidas necessárias;
- continuar a desenvolver um serviço de reputação de endereços IP para proteger os serviços digitais do governo (com isso, os serviços online poderão obter informações sobre um endereço IP que se conecte a eles, contribuindo para a tomada de decisões mais bem informadas em tempo real nas atividades de gerenciamento de riscos);
- instalar produtos nas redes governamentais que verifiquem se os *softwares* estão funcionando corretamente, sem interferência maliciosa;
- procurar expandir os esforços para além do domínio do portal GOV.UK, introduzindo outros serviços digitais que notifiquem os usuários que estejam utilizando navegadores desatualizados; e
- investir em tecnologias como os Trusted Platform Modules (TPM) e em padrões emergentes no setor, como o Fast Identity Online (FIDO), que não dependam de senhas para a autenticação de usuários, utilizando-se a própria máquina e outros dispositivos na posse do usuário para autenticá-lo. O governo realizará testes com mecanismos de autenticação inovadores para demonstrar seus benefícios, tanto em termos de segurança quanto em relação à experiência global do usuário.

5.2.6. O governo também buscará novas formas de incentivo ao mercado, criando classificações de segurança para novos produtos para que o consumidor tenha informações claras sobre os produtos e serviços que lhe ofereçam maior segurança. O governo buscará, ainda, novas formas de vincular essas classificações aos órgãos existentes ou aos que venham a ser criados, assim como novos meios de alertar os consumidores antes que lancem alguma ação online capaz de comprometer sua segurança.

Avaliação dos resultados

5.2.7. O êxito do governo em fortalecer a segurança da Internet será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- a maioria dos produtos e serviços comerciais disponíveis no Reino Unido em 2021 deve contribuir para tornar o país mais seguro por possuir recursos de segurança habilitados por padrão ou integrados em sua concepção; e
- Todos os serviços públicos prestados a nível nacional, local e das Administrações Regionais terão a confiança do público por serem implementados com o maior grau de segurança possível e por estarem os níveis de fraude dentro de parâmetros de risco aceitáveis.

5.3. PROTEÇÃO AO GOVERNO

5.3.1. O governo britânico, as Administrações Regionais e o setor público em geral detêm grandes quantidades de dados sigilosos. Prestam serviços essenciais à população e operam redes críticas para a segurança e resiliência nacional. Os sistemas do governo sustentam o funcionamento da nossa sociedade. A modernização dos serviços do setor público continuará a constituir a base da Estratégia Digital do Reino Unido: a ambição

digital do Governo é que o país seja líder no mundo enquanto nação digital.
Para manter a confiança da população nos serviços e sistemas públicos online, os dados detidos pelo governo devem estar protegidos e todas as repartições públicas devem assegurar níveis adequados de segurança cibernética face às contínuas tentativas de atores hostis de obter acesso ao governo e às redes e dados do setor público.

Objetivos

5.3.2. Pretendemos alcançar os resultados a seguir:

- A população deve ter confiança nos serviços públicos online: deve confiar que suas informações confidenciais estão seguras e, de sua parte, entender a sua responsabilidade por transmitir suas informações sigilosas de maneira segura;
- O governo deve definir e adotar padrões de segurança cibernética adequados, assegurando que todas as repartições públicas entendam e cumpram sua obrigação de proteger suas redes, dados e serviços; e
- Os ativos críticos do governo, sobretudo aqueles enquadrados na classificação mais elevada, devem estar protegidos contra ataques cibernéticos.

Nossa abordagem

5.3.3. O governo continuará a inserir mais de seus serviços no meio eletrônico, para que o Reino Unido se torne de fato um país "digital por padrão". O Government Digital Service (GDS), o Crown Commercial Service (CCS) e o NCSC serão responsáveis por assegurar que todos os novos serviços digitais desenvolvidos ou contratados pelo governo também sejam "seguros por padrão".

5.3.4. As redes públicas são altamente complexas e, em muitos casos, ainda integram sistemas legados, assim como *softwares* comercias para os quais os fornecedores deixaram de oferecer suporte. Será garantido que não haja riscos a descoberto oriundos de sistemas legados e *softwares* não suportados.

5.3.5. Será fortalecida a resiliência do governo e do setor público em geral contra ataques cibernéticos. Para isso, será necessário garantir a manutenção de informações precisas e atualizadas sobre todos os sistemas, dados e sobre quem pode acessá-los. A probabilidade e o impacto de um incidente cibernético serão minimizados através da implementação das melhores práticas estabelecidas pelo NCSC.
O governo também deverá garantir a sua capacidade de resposta a incidentes cibernéticos através de um programa de simulados de incidentes e testes periódicos das redes públicas. As Administrações Regionais e autoridades locais serão convidadas a participar desses simulados, conforme for o caso. Através de varreduras automatizadas, será feito um diagnóstico mais preciso do estado de segurança online do governo.

5.3.6. A segurança cibernética não é apenas uma questão tecnológica. Quase todos os ataques cibernéticos bem-sucedidos têm a contribuição de fatores humanos. Portanto, dar-se-á continuidade aos investimentos destinados aos servidores públicos, garantindo que todos estejam adequadamente conscientizados do risco cibernético. Serão desenvolvidos conhecimentos cibernéticos específicos em áreas onde os riscos sejam maiores, e será assegurada a existência de processos adequados ao controle eficaz desses riscos.

5.3.7. Ao NCSC caberá formular orientações de segurança cibernética que acompanhem a evolução das ameaças e o desenvolvimento de novas tecnologias. Serão tomadas medidas para garantir que as organizações governamentais tenham fácil acesso a informações sobre ameaças para que possam entender seus próprios riscos cibernéticos e tomar medidas adequadas a respeito.

5.3.8. Continuaremos a fortalecer as redes enquadradas nas classificações de risco mais elevadas para salvaguardar as comunicações mais sigilosas do governo.

5.3.9. Os sistemas de saúde e assistência social apresentam desafios únicos no contexto da

segurança cibernética. O setor emprega cerca de 1,6 milhão de pessoas em mais de 40 mil organizações, cada uma com recursos e estruturas de segurança da informação muito distintos. O National Data Guardian, voltado à Saúde e Assistência Social, definiu novos padrões de segurança de dados para o setor na Inglaterra, além de um novo modelo do termo de consentimento/não consentimento ao fornecimento de dados por pacientes. O governo atuará junto às organizações de saúde e de assistência social na implementação dessas normas.

"A Grã-Bretanha é líder mundial em segurança cibernética, mas com a escalada das ameaças, o novo Centro de Operações de Segurança Cibernética será fundamental para garantir que nossas Forças Armadas possam continuar a operar com segurança. O aumento do orçamento de defesa permitirá ficar à frente dos nossos adversários no ciberespaço, além de contemplar investimentos em recursos convencionais"

Michael Fallon,
Secretário de Defesa, abril de 2016

5.3.10. A segurança cibernética é vital para nossa defesa. Nossas Forças Armadas dependem de sistemas de informação e comunicação tanto no Reino Unido quanto em suas operações mundo afora. As infraestruturas e o pessoal do Ministério da Defesa (MoD) estão entre os principais alvos de ataques. Os sistemas de defesa são frequentemente alvo de ataques de criminosos, serviços de inteligência estrangeiros e outros atores maliciosos que visam a exploração de seu pessoal, a interferência em suas atividades e operações, e o corrompimento e furto de informações. Serão intensificadas as ações de conscientização, detecção e resposta a ameaças cibernéticas através da criação de um Centro de Operações de Segurança Cibernética (CSOC) dotado de tecnologias cibernéticas defensivas de última geração para proteger o ciberespaço do Ministério da Defesa e tratar de ameaças. O CSOC atuará em estreita articulação com o NCSC na superação dos desafios de segurança cibernética enfrentados pelo Ministério da Defesa, contribuindo para o fortalecimento da segurança cibernética nacional.

Avaliação dos resultados

5.3.11. O êxito do governo em proteger suas redes, sistemas e dados será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- o governo conhecer profundamente o nível de risco à segurança cibernética em todo o governo e no setor público em geral;
- todas as repartições públicas e outros órgãos protegerem-se proporcionalmente ao seu nível de risco e segundo um padrão mínimo definido para o setor público;
- as diversas repartições da administração pública e o setor público em geral serem resilientes e capazes de responder com eficácia a incidentes cibernéticos, mantendo suas funções e se recuperando com rapidez;
- as novas tecnologias e serviços digitais implantados pelo governo serem dotados de segurança cibernética integrada por padrão;
- o governo ter conhecimento e mitigar ativamente todas as vulnerabilidades conhecidas da Internet nos sistemas e serviços públicos; e
- todos os fornecedores do governo atenderem às normas de segurança cibernética definidas.

5.4. PROTEÇÃO ÀS INFRAESTRUTURAS CRÍTICAS NACIONAIS E OUTROS SETORES PRIORITÁRIOS

Contexto

5.4.1 A segurança cibernética de determinadas organizações do Reino Unido é de particular importância, uma vez que um ataque cibernético bem-sucedido a essas organizações teria maior impacto na segurança nacional do país. Esse impacto pode ter influência no cotidiano dos cidadãos britânicos, na estabilidade e na força da economia britânica, ou na reputação e imagem internacional do país. Nesse grupo de empresas e organizações dos setores público e privado estão aquelas representativas das infraestruturas críticas (IEC) nacionais e que prestam serviços essenciais à nação. Garantir a segurança e resiliência das IEC contra ataques cibernéticos

será uma prioridade para o governo. Esse grupo também inclui outras empresas e organizações, além das IEC, que exijam um maior nível de suporte. São elas:

- as joias da nossa coroa econômica: as empresas mais bem-sucedidas do Reino Unido e que sustentam a nossa força econômica futura pelo valor de sua produção científica e propriedade intelectual;
- empresas e organizações detentoras de dados: não apenas organizações que detêm grandes quantidades de dados pessoais, mas também aquelas que detêm dados sobre cidadãos vulneráveis no país e no exterior, como entidades filantrópicas;
- alvos mais sujeitos a ameaças: como veículos de comunicação, uma vez que ataques a essas organizações podem prejudicar a reputação do Reino Unido, a confiança pública no governo ou a liberdade de expressão;
- as empresas que formam a base da economia digital: empresas prestadoras de serviços digitais que viabilizam o comércio eletrônico e a nossa economia digital e que dependem da confiança dos consumidores nos seus serviços; e
- organizações que, através das forças do mercado e por serem autoridades no assunto, sejam capazes de exercer influência sobre a economia global e fortalecer a segurança cibernética, como seguradoras, investidores, reguladores e consultorias.

5.4.2. É preciso fazer mais para proteger esses elementos vitais da nossa economia e apoiar as organizações que exercem forte influência sobre as demais. Nossas IEC, tanto no setor privado quanto no público, continuam sendo alvo de ataques. Nesses e em outros setores prioritários, ainda não há uma conscientização e controle adequado do risco cibernético, enquanto as ameaças continuam a se diversificar e proliferar.

Objetivo

5.4.3. O Governo do Reino Unido deve atuar, em colaboração com as administrações regionais e outras autoridades competentes, quando for o caso, a fim de garantir que as organizações e empresas mais importantes do Reino Unido, incluindo as IEC, tenham segurança e resiliência adequada face aos ataques cibernéticos. Nem o governo nem outros órgãos públicos assumirão a responsabilidade de controlar esses riscos a favor do setor privado, responsabilidade esta que recai na administração e nos operadores das respectivas empresas. Entretanto, o governo está comprometido em dar apoio e garantias de segurança proporcionais à ameaça enfrentada por essas empresas e organizações e às possíveis consequências de ataques.

"A segurança cibernética é fundamental para viabilizar a inovação e o crescimento. Com a criação de organizações específicas e adoção de uma abordagem centrada nos riscos à segurança cibernética, as organizações poderão voltar suas atenções às oportunidades e à exploração. A confiança nas empresas atuantes no segmento de Internet das Coisas (IoT), e que apoiam e protegem o consumidor e seus dispositivos móveis pessoais (desde aparelhos de celular até dispositivos médicos, aparelhos inteligentes e carros inteligentes), é um importante diferencial competitivo e deve ser priorizado."

EY, Pesquisa Global da Segurança da Informação 2015

Nossa abordagem

5.4.4. Cabe às organizações e a administração das empresas garantir a segurança de suas redes. Devem identificar seus sistemas críticos e avaliar periodicamente sua vulnerabilidade diante da constante evolução tecnológica e das ameaças. Devem investir em tecnologia e em seus colaboradores para reduzir as vulnerabilidades nos sistemas atuais e futuros e em sua cadeia de suprimentos, mantendo um nível de segurança cibernética proporcional ao risco. Também devem contar com estruturas previamente testadas para responder a um eventual ataque. No caso das IEC, devem atuar de forma colaborativa com órgãos governamentais e reguladores para assegurar que o risco cibernético seja adequadamente controlado e, caso não seja, intervir no interesse da segurança nacional.

5.4.5. Portanto, caberá ao governo entender o nível de segurança cibernética nas IEC e adotar medidas para intervir, quando necessário, para promover melhorias de interesse nacional.

5.4.6. Nesse sentido, compete ao governo:

- difundir aos atores do setor privado informações sobre ameaças acessíveis somente ao governo, para que possam antecipar-se a elas;
- emitir diretrizes sobre o controle de riscos cibernéticos e, em parceria com o setor privado e o meio acadêmico, definir boas práticas de segurança cibernética;
- incentivar a introdução de recursos de segurança de ponta para a proteção das IEC, como instalações de treinamento, laboratórios de testes, normas de segurança e serviços de consultoria; e
- realizar simulados junto às IEC para auxiliá-los na gestão de riscos cibernéticos e vulnerabilidades.

5.4.7. O NCSC será responsável por fornecer esses serviços às empresas e organizações mais críticas do Reino Unido, inclusive às IEC. Para isso, atuará em parceria com departamentos do governo e reguladores, aos quais caberá assegurar que os riscos cibernéticos sejam gerenciados em seus setores segundo os padrões exigidos por interesses nacionais.

5.4.8. Será também atribuição do governo assegurar a adoção de um marco regulatório adequado para a segurança cibernética, que:

- garanta que o setor privado atue para se proteger das ameaças;
- tenha por objeto os resultados almejados e seja suficientemente flexível, evitando que se torne obsoleto diante da evolução das ameaças ou que vise apenas o cumprimento legal, e não a boa gestão dos riscos;
- tenha a agilidade necessária para fomentar, mas não protagonizar, o crescimento e a inovação;
- esteja harmonizado com os regimes de outras jurisdições, de modo que as empresas britânicas não sejam oneradas por uma abordagem fragmentada e heterogênea; e
- ofereça, quando associado ao apoio efetivo do governo, uma vantagem competitiva para o Reino Unido.

5.4.9. Muitos de nossos setores industriais já são regulamentados em matéria de segurança cibernética. No entanto, temos de garantir a tomada de medidas adequadas em toda a economia, inclusive nas IEC, para gerir os riscos à segurança cibernética.

Avaliação dos resultados

5.4.10. O êxito do governo em proteger nossas IEC e outros setores prioritários será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- o governo conhecer o nível de segurança cibernética nas IEC e adotar medidas para intervir, quando necessário, para promover melhorias de interesse nacional.
- nossas empresas e organizações mais importantes estarem conscientizadas quanto ao nível da ameaça e adotarem práticas proporcionais de segurança cibernética.

5.5. MUDANÇA DE COMPORTAMENTO NA POPULAÇÃO E NAS EMPRESAS

5.5.1 O sucesso da economia digital no país depende da confiança das empresas e da população nos serviços eletrônicos. O governo do Reino Unido tem atuado junto ao setor privado e outros segmentos do setor público para aumentar a conscientização e compreensão das ameaças. O governo também proporcionou à população e às empresas o acesso a alguns dos recursos necessários para sua proteção. Embora existam muitas organizações que já atuam com excelência na proteção cibernética e na prestação de serviços online, estando algumas entre as líderes mundiais no tema, – a maioria das empresas e da população ainda não pratica uma gestão adequada dos riscos cibernéticos.

"No ano passado, o custo médio das violações de segurança em grandes empresas foi de £ 36.500. Nas pequenas empresas, o custo médio foi de £

3.100. 65% das grandes organizações relataram ter sofrido ao menos uma violação de segurança da informação no ano passado e, dessas, 25% sofreram uma violação pelo menos uma vez por mês. Quase sete entre dez ataques envolveram vírus, *spywares* ou *malwares* que poderiam ter sido evitados com a adoção do programa Cyber Essentials, do governo do Reino Unido."

2016 Government Cyber Health Check and Cyber Security Breaches Survey

Objetivo

5.5.2. Nosso objetivo visa garantir que a população e as organizações, independentemente de seu porte ou do setor, tomem medidas adequadas para protegerem a si e aos seus clientes contra os danos causados por ataques cibernéticos.

Nossa abordagem

5.5.3. Será atividade do governo difundir orientações para a proteção da economia. Aperfeiçoaremos a forma de divulgação dessas orientações para maximizar seus efeitos. Para a população, o governo recorrerá a autoridades no assunto para aumentar o alcance, credibilidade e relevância da nossa mensagem. Serão formuladas orientações que sejam fáceis de aplicar e relevantes para os usuários no ponto de acesso aos serviços e de exposição aos riscos. Serão envolvidas as Administrações Regionais e outras autoridades, conforme apropriado.

5.5.4. Para as empresas, nossa atuação se dará através de organizações como seguradoras, reguladores e investidores capazes exercer influência nas empresas para que adotem práticas adequadas de gestão de riscos cibernéticos. Nesse sentido, destacaremos os nítidos benefícios do ponto de vista econômico e o custo do risco cibernético na avaliação de formadores de opinião. Procuraremos melhor entender os fatos que impediram muitas organizações de se protegerem adequadamente. Munidos dessas informações, trabalharemos em parceria com organizações, como entidades de normatização, para irmos além da mera conscientização e convencer as empresas a agirem a respeito. Também será assegurada a existência de um marco regulatório adequado para gerir os riscos cibernéticos não tratados pelo mercado. Nesse âmbito, o governo recorrerá a instrumentos como o GDPR para elevar os padrões de segurança cibernética e proteger o cidadão.

5.5.5. A população e as organizações do Reino Unido terão acesso às informações, conhecimentos e recursos necessários à sua proteção. Para promover a transformação necessária nos comportamentos de segurança da população, haverá uma comunicação harmonizada e coerente de orientações de segurança cibernética, tanto por parte do governo quanto por parte de seus parceiros. Ao NCSC caberá publicar orientações técnicas nesse sentido. Estas deverão refletir as prioridades e as práticas dos setores público e privado, devendo também ser claras, facilmente acessíveis e coerentes, além de acompanhar a evolução das ameaças. A polícia trabalhará em estreita colaboração com o setor privado e o NCSC, divulgando informações atualizadas de inteligência sobre ameaças criminais, apoiando o setor privado para que este possa se defender contra ameaças, e mitigando o impacto de ataques contra vítimas no Reino Unido.

Avaliação dos resultados

5.5.6. O êxito do governo em proteger nossas IEC e outros setores prioritários será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- o nível de segurança cibernética da economia britânica ser igual ou superior ao das economias avançadas comparáveis;
- o número, a gravidade e o impacto dos ataques cibernéticos bem-sucedidos contra empresas no Reino Unido se reduzir como consequência das melhorias em higiene cibernética; e
- serem registradas melhorias na cultura de segurança cibernética no Reino Unido, fruto da maior conscientização das organizações e da população sobre os níveis de risco cibernético e as medidas de higiene cibernética que devem tomar para geri-los.

CYBER AWARE

A campanha *Cyber Aware*, anteriormente denominada *Cyber Streetwise*, traz à população as diretrizes necessárias para se protegerem de cibercriminosos. Mensagens dirigidas, veiculadas por meio das redes sociais e peças publicitárias, em parceria com a iniciativa privada, promovem:

- o uso de três palavras aleatórias para criar senhas fortes; e
- o hábito de sempre baixar as atualizações de *software* mais recentes.

Especialistas concordam que a adoção desses comportamentos é capaz de proteger as pequenas empresas e a população contra crimes cibernéticos. A campanha *Cyber Aware* atualmente conta com o apoio de 128 parceiros de diversos setores, incluindo a polícia e empresas dos setores de varejo, lazer, viagens e serviços profissionais. Em 2015/16, estima-se que 10 milhões de adultos e 1 milhão de pequenas empresas tenham manifestado a intenção de manter ou adotar comportamentos de segurança cibernética como consequência da campanha *Cyber Aware*.

Para saber mais, acesse cyberaware.gov.uk

CYBER ESSENTIALS

O programa *Cyber Essentials* foi criado com o objetivo de ensinar as organizações a se protegerem contra ameaças de baixo nível, porém com altos índices de difusão. São destacados cinco controles técnicos (controle de acesso, *firewalls* e *gateways* de Internet, proteção contra *malwares*, gerenciamento de *patches* e configurações de segurança) que as organizações devem adotar. A grande maioria dos ataques cibernéticos utiliza métodos relativamente simples, que exploram vulnerabilidades básicas em *softwares* e sistemas de informática. Existem ferramentas e técnicas amplamente disponíveis na Internet que permitem que até mesmo atores sem maiores habilidades explorem essas vulnerabilidades. A correta implementação do *Cyber Essentials* garante a proteção contra a grande maioria das ameaças mais comuns na Internet.

5.6. TRATANDO DE INCIDENTES E ENTENDENDO A AMEAÇA

5.6.1. A expectativa é de haver aumento na incidência e na gravidade dos incidentes cibernéticos que atingem organizações nos setores público e privado. Portanto, é preciso definir a forma como os setores privado e público devem interagir com o governo na ocorrência de um incidente cibernético. O nível de apoio a ser oferecido pelo governo do Reino Unido para cada setor, tendo em conta sua maturidade cibernética, deve ser claramente definido e compreendido. A coleta e divulgação pelo governo de informações sobre ameaças deve ser feita de forma e com agilidade adequada aos diversos tipos de organização. O setor privado, o governo e a população têm atualmente acesso a diversas fontes de informação, orientação e assistência em matéria de segurança cibernética. Esse acesso deve ser simplificado.

5.6.2. Devemos assegurar que a atuação do Governo, tanto na resposta a incidentes quanto na divulgação de diretrizes, não ocorra de forma isolada, mas sim em parceria com o setor privado. Nossos processos de tratamento de incidentes devem utilizar uma abordagem holística, baseada no aprendizado e no intercâmbio de técnicas de mitigação com nossos parceiros. A articulação com outras equipes de resposta a emergências informáticas (*Computer Emergency Response Teams – CERTs*) e com nossos aliados também continuará a ser parte integrante das atividades de resposta e tratamento de incidentes.

5.6.3. O tratamento de incidentes ainda é um processo fragmentado entre os diversos departamentos governamentais, pelo que a presente estratégia prevê a criação de uma abordagem unificada. O NCSC será responsável por oferecer um serviço de resposta a incidentes eficiente e eficaz, coordenado pelo governo. Na ocorrência de um incidente cibernético de grande dimensão, as Forças Armadas estarão aptas a prestar assistência, seja de forma convencional, tratando do impacto físico do incidente, ou sob a forma de apoio cibernético especializado prestado por militares da ativa ou reservistas. Embora o governo se comprometa a prestar todo o apoio possível com os meios à sua disposição, cabe salientar a importância da atuação do próprio setor privado, da sociedade e da população para assegurar sua segurança cibernética básica.

Objetivos

5.6.4. Dentre os nossos objetivos, destacam-se os seguintes:

- o Governo adotará uma metodologia harmonizada e integrada no tratamento de incidentes, a partir de uma melhor compreensão e conhecimento das ameaças e ações promovidas contra o país. Será de fundamental importância a atuação do NCSC como viabilizador do processo, assim como a parceria com o setor privado, as polícias e outros órgãos, autoridades e agências públicas;
- O NCSC deve definir processos claros para a comunicação de incidentes, adaptados ao perfil da vítima; e
- Devemos atuar para prevenir os incidentes cibernéticos mais comuns, adotando estruturas eficazes de difusão de informações para instruir o planejamento "pré-incidente".

Nossa abordagem

5.6.5. Cabe à administração das organizações e das empresas, tanto do setor público quanto do privado, garantir a segurança de suas redes e realizar exercícios de simulação de seus planos de resposta a incidentes. Na ocorrência de um incidente de grande dimensão, o processo de tratamento de incidentes adotado pelo governo deve contemplar os três elementos de um incidente cibernético: as causas precursoras, o próprio incidente e a resposta pós-incidente.

5.6.6. Para que o tratamento de incidentes seja eficaz tanto para o governo quanto para o setor privado, atuaremos de forma colaborativa na revisão e definição do escopo da resposta do governo, intensificando a cooperação. Será ampliado o plano nacional de exercícios

cibernéticos, a partir da nossa melhor compreensão e conhecimento das ameaças, aprimorando o apoio oferecido a parceiros dos setores público e privado.

5.6.7. Criaremos um órgão governamental revestido de fé pública e credibilidade para prestar assistência e orientações em matéria de incidentes. Sua atuação permitirá elevar a conscientização da segurança cibernética na comunidade digital do Reino Unido, identificar, com maior clareza, as tendências emergentes, tomar medidas proativas e, dessa forma, evitar a ocorrência de incidentes.

5.6.8. A transição para a difusão automatizada de informações (ou seja, sistemas de segurança cibernética capazes de emitir automaticamente alertas uns aos outros sobre incidentes ou ataques) permitirá oferecer um serviço mais eficaz. Com isso, as organizações poderão agir com maior agilidade conforme as informações recebidas sobre ameaças.

Avaliação dos resultados

5.6.9. O êxito do Governo no tratamento de incidentes será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- uma maior proporção dos incidentes ser comunicada às autoridades, levando a uma melhor compreensão da dimensão e escala das ameaças;
- tratamento mais eficaz, eficiente e abrangente dos incidentes cibernéticos, fruto da criação do NCSC como mecanismo centralizado de notificação e resposta a incidentes; e
- abordarmos as causas-raiz dos ataques a nível nacional, reduzindo a ocorrência de ataques repetidos às mesmas vítimas e setores.

6. DISSUADIR

6.0.1. De acordo com a Estratégia de Segurança Nacional, a defesa e a proteção começam com a dissuasão. Isso é verdade tanto no ciberespaço quanto em qualquer outra esfera. Para concretizar a nossa visão de sermos uma nação ao mesmo tempo segura e resiliente às ameaças cibernéticas e próspera e confiante no mundo digital, é preciso dissuadir aqueles que tentem prejudicar a nós e os nossos interesses. Para isso, é necessário que todos continuem a elevar os níveis de segurança cibernética, de modo que qualquer tentativa de ataque no ciberespaço, seja para fins de furto de informações ou para nos prejudicar de outra forma, seja dificultado e custe caro para o infrator. Nossos adversários devem saber que não poderão agir com impunidade: que podemos e iremos identificá-los, e que somos capazes de combatê-los com a resposta mais adequada entre os diversos recursos à nossa disposição. Continuaremos a construir alianças internacionais e a promover a aplicação do direito internacional no ciberespaço. Seremos também mais ativos em desarticular as atividades daqueles que nos ameaçam no ciberespaço e a infraestrutura que utilizam. A concretização dessa ambição requer recursos soberanos de classe mundial.

6.1. O PAPEL CIBERNÉTICO NA DISSUASÃO

6.1.1. O ciberespaço é apenas uma das esferas em que devemos defender nossos interesses e soberania. Assim como as nossas ações na esfera física têm efeito na segurança e capacidade de dissuasão no meio cibernético, também as nossas ações e posturas no ciberespaço devem contribuir para a segurança nacional global.

6.1.2. Os princípios de dissuasão aplicam-se no ciberespaço da mesma forma que na esfera física. O Reino Unido deixa claro que todo o arsenal de recursos a seu dispor será utilizado para dissuadir os adversários e negar-lhes a oportunidade de nos atacar. No entanto, reconhecemos que a segurança cibernética e a resiliência são, em si, um meio de dissuadir os ataques que dependem da exploração de vulnerabilidades.

6.1.3. Será adotada uma abordagem abrangente de segurança e dissuasão cibernética, que torne o Reino Unido um alvo mais difícil de ser atingido, reduzindo os benefícios e aumentando o encargo para os nossos adversários, sejam eles políticos, diplomáticos, econômicos ou estratégicos. O país deve deixar claro para possíveis adversários a sua capacidade e intenção de responder, influenciando suas decisões. Teremos os recursos e instrumentos necessários para: negar aos nossos adversários oportunidades fáceis para comprometer as nossas redes e sistemas; conhecer sua intenção e capacidade; frustrar a ação dos *malwares* empregados em larga escala; e responder e proteger a nação no ciberespaço.

6.2. REDUÇÃO DA CRIMINALIDADE CIBERNÉTICA

6.2.1. É preciso elevar a onerosidade e os riscos, e reduzir as recompensas, da atividade cibercriminosa. Paralelamente aos esforços para fortalecer o Reino Unido contra ataques cibernéticos e reduzir suas vulnerabilidades, devemos também focar incansavelmente em criminosos que continuarem atacando o Reino Unido.

6.2.2. As agências policiais irão focar seus esforços para deter os criminosos que persistem em atacar a população e as empresas do país. Trabalharemos com parceiros nacionais e internacionais para perseguir os criminosos onde quer que estejam e desmantelar suas infraestruturas e redes de facilitação. As agências policiais também atuarão na conscientização e na elevação dos padrões de segurança cibernética, em colaboração com o NCSC.

6.2.3. Esta estratégia complementa a Estratégia de Combate a Crimes Graves e Organizados de 2013, que estabelece a resposta estratégica adotada pelo governo do Reino Unido contra a cibercriminalidade, além de outros crimes graves e organizados. A National Cyber Crime Unit (NCCU), vinculada à Agência Nacional de Combate ao Crime (NCA), foi criada com o objetivo de coordenar a resposta nacional ao crime cibernético. A *Action Fraud* atua como

centro nacional para a comunicação de fraudes e crimes cibernéticos. Uma rede de unidades especializadas de combate à cibercriminalidade, que integram as Unidades Regionais de Combate ao Crime Organizado (ROCUs), disponibiliza recursos especializados a nível regional em apoio à NCCU e às forças policiais locais.

Objetivo

6.2.4. Reduziremos os impactos do crime cibernético no Reino Unido e nos seus interesses pela dissuasão dos criminosos cibernéticos e pela perseguição insistente implacável àqueles que persistem em nos atacar.

Nossa abordagem

6.2.5. A fim de reduzir o impacto dos crimes cibernéticos, devemos:

- fortalecer as estruturas e a capacidade de fiscalização do Reino Unido a nível nacional, regional e local, a fim de identificar, perseguir, trazer à justiça e dissuadir os cibercriminosos no Reino Unido e no exterior;
- aprofundar nossos conhecimentos sobre o modelo de negócios do crime cibernético, para que possamos dirigir as intervenções de modo a causarem maiores efeitos na desarticulação da atividade criminosa. Usaremos esses conhecimentos para:
  - tornar o Reino Unido um ambiente em que a atividade criminosa apresente elevada onerosidade e risco, atingindo os focos de criminalidade no país e trabalhando com o setor privado para reduzir a capacidade dos criminosos de explorar a infraestrutura nacional; e
  - combater a cibercriminalidade em sua origem, dificultando o modelo de negócios dos criminosos através da desarticulação de suas infraestruturas e redes financeiras e, sempre que possível, levando os infratores à justiça.

- criar parcerias internacionais para combater a percepção de impunidade dos cibercriminosos localizados no exterior que pratiquem crimes contra o Reino Unido, levando-os à justiça;

- dissuadir aqueles que sejam atraídos ou pretendam se envolver na cibercriminalidade, através das medidas já existentes de intervenção antecipada;
- ampliar as parcerias com o setor privado, para que o governo forneça informações de inteligência sobre ameaças ao setor privado, e este nos forneça informações de inteligência na origem, subsidiando nossos esforços para deter o crime cibernético em sua gênese;
- criar no âmbito da *Action Fraud* uma nova estrutura de comunicação e triagem de incidentes com atendimento 24 horas, articulada com o NCSC, a Unidade Nacional de Cibercriminalidade da ANC e a comunidade policial, visando melhorar o apoio oferecido às vítimas de cibercrimes, garantir uma resposta mais rápida aos crimes comunicados e oferecer orientações mais úteis sobre segurança e proteção. Será criado um novo sistema de comunicação para a difusão em tempo real, entre agências policiais, de informações sobre cibercrimes e ameaças;
- atuar junto ao NCSC e ao setor privado para reduzir as vulnerabilidades na infraestrutura do Reino Unido que possam ser exploradas em larga escala por cibercriminosos; e
- atuar junto ao setor financeiro para tornar o Reino Unido um ambiente mais hostil àqueles que pretendam monetizar o roubo de identidade, inclusive pela desarticulação de suas redes.

Avaliação dos resultados

6.2.6. O êxito do governo em reduzir o crime cibernético será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- maior capacidade de desarticulação dos criminosos cibernéticos que promovam ataques ao Reino Unido, evidenciada pelo aumento das prisões e condenações e por um número maior de redes criminosas desarticuladas como consequência das intervenções dos órgãos policiais;

- maior capacidade de fiscalização, incluindo um aumento da capacidade e das competências tanto dos órgãos policiais especializados quanto dos convencionais, e uma maior capacidade de fiscalização junto a parceiros estrangeiros;
- aumento da eficácia e da extensão das medidas de intervenção precoce, dissuadindo e reabilitando possíveis infratores; e
- redução das infrações cibernéticas de baixa complexidade pela dificultação do acesso e menor eficácia dos serviços cibernéticos criminosos.

ORIENTAÇÕES PARA VÍTIMAS DE CRIMES CIBERNÉTICOS

Se você acredita ter sido vítima de um crime cibernético, ou de um golpe praticado com auxílio de recursos cibernéticos, deve entrar em contato com o serviço *Action Fraud*.

Para comunicar o ocorrido, use a ferramenta online de comunicação de fraudes do serviço *Action Fraud* a qualquer hora do dia ou da noite, ou ligue para o número 0300 123 2040. Para outras informações, acesse www.actionfraud.police.uk

O serviço *ActionFraud* é mantido pela Polícia Municipal de Londres.

6.3. COMBATE A ATORES ESTRANGEIROS HOSTIS

6.3.1. Devemos lançar mão de todo o arsenal à disposição do governo para combater os perigos representados por atores estrangeiros hostis, cuja ameaça à nossa segurança política, econômica e militar aumenta a cada dia. As parcerias internacionais serão fundamentais para o nosso êxito nesse sentido. Assim, será dada maior ênfase à articulação e trabalho em conjunto com esses parceiros no combate às ameaças. Grande parte dessa atuação se dará externamente ao domínio público. Os investimentos em nossa capacidade soberana e em parcerias com o setor privado continuarão a ser fundamentais para a nossa capacidade de detectar, observar e identificar ameaças, que estão em constante evolução.

Objetivo

6.3.2. Estabeleceremos estratégias, políticas e prioridades para cada adversário, garantindo uma abordagem proativa, bem equacionada e eficaz no combate às ameaças e reduzindo o número e a gravidade dos incidentes cibernéticos no futuro.

Nossa abordagem

6.3.3. De modo a reduzir a ameaça cibernética de atores estrangeiros hostis, devemos:

- reforçar a aplicação do direito internacional no ciberespaço, além de promover acordos para a adoção de normas voluntárias e não vinculativas que visem o comportamento responsável de Estados e a formulação e implementação de medidas para o fortalecimento da confiança;
- trabalhar com parceiros internacionais, sobretudo através da defesa coletiva, da segurança cooperativa e da maior capacidade de dissuasão proporcionada pela nossa participação na OTAN;
- identificar os aspectos específicos e genéricos das atividades cibernéticas de nossos adversários;
- identificar e explorar todas as opções disponíveis para a dissuasão e combate a essa ameaça, utilizando para isso todo o leque de recursos a dispor do governo. Serão contemplados outros fatores relacionados, como as estratégias específicas para determinados países, prioridades cibernéticas internacionais e objetivos relacionados à criminalidade cibernética e à prosperidade;
- utilizar as redes e relações existentes com nossos principais parceiros internacionais para o intercâmbio de informações sobre ameaças atuais e emergentes, agregando valor aos conhecimentos e experiência existentes; e
- divulgar identidades cibernéticas específicas quando tal for considerado de interesse nacional.

Avaliação dos resultados

6.3.4. O êxito do governo em combater as ações hostis de atores estrangeiros será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

• consolidação de redes de intercâmbio de informações com nossos parceiros internacionais e acordos multilaterais ampliados para a promoção de condutas lícitas e responsáveis por parte dos Estados, contribuindo substancialmente para a nossa capacidade de entender e responder às ameaças e fortalecendo as defesas do Reino Unido; e
• existência de medidas de defesa e dissuasão aliadas a estratégias específicas por país, tornando o Reino Unido um alvo mais difícil de ser atingido por atores estrangeiros hostis.

6.4. PREVINIENDO TERRORISMO

6.4.1. Embora a capacidade técnica das organizações terroristas continue limitada, estas ainda ambicionam conduzir atividades danosas ao Reino Unido através das redes de computadores, sendo a visibilidade e a perturbação da ordem os principais objetivos de suas atividades cibernéticas. Cabe ao governo identificar e desarticular os terroristas que utilizem ou pretendam utilizar o meio cibernético para tais fins. Dessa forma, será possível minimizar o impacto e evitar o aumento da capacidade cibernética dos terroristas, aumento este que traria maiores ameaças às redes e à segurança nacional do Reino Unido.

Objetivo

6.4.2. Mitigar a ameaça do uso do espaço cibernético por terroristas, através da identificação e desarticulação dos atores terroristas que atualmente tenham ou ambicionem desenvolver a capacidade de ameaçar a segurança nacional do Reino Unido.

Nossa abordagem

6.4.3. Para que a ameaça representada pelo terrorismo cibernético continue baixa, devemos:

- detectar ameaças de terrorismo cibernético, identificando os atores que busquem conduzir nas redes atividades danosas ao Reino Unido e aos seus aliados;
- investigar e desarticular esses atores do terrorismo cibernético, impedindo-os de fazer uso de recursos cibernéticos contra o Reino Unido e seus aliados; e
- trabalhar em estreita colaboração com parceiros internacionais para que a ameaça do terrorismo cibernético seja enfrentada da melhor maneira.

Avaliação dos resultados

6.4.4. O êxito do governo na prevenção do terrorismo será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- uma perfeita compreensão do risco representado pelo ciberterrorismo, através da identificação e investigação de ameaças de terrorismo cibernético ao Reino Unido; e
- vigilância e desarticulação precoce das estruturas cibernéticas de terroristas, impedindo o aumento da capacidade de organizações terroristas a longo prazo.

6.5. AUMENTO DA CAPACIDADE SOBERANA – CAPACIDADE CIBERNÉTICA OFENSIVA

6.5.1. A capacidade cibernética ofensiva permite a intrusão proposital nos sistemas ou redes de adversários a fim de provocar danos, interferências ou destruição. Integra o arsenal de recursos a serem desenvolvidos para dissuadir nossos adversários e negar-lhes a oportunidade de nos atacar, tanto no ciberespaço quanto na esfera física. Por meio do Programa Nacional de Ação Cibernética Ofensiva (NOCP), contamos com uma estrutura específica voltada à atuação no ciberespaço, e serão destinados recursos para desenvolver e aprimorá-la.

Objetivo

6.5.2. Devemos ter à nossa disposição uma capacidade cibernética ofensiva adequada que possa ser acionada em um momento e local oportunos, para fins tanto dissuasivos como

operacionais, sempre de acordo com a legislação nacional e internacional.

Nossa abordagem

6.5.3. Para isso, prevê-se:

- investir no NOCP, uma parceria entre o Ministério da Defesa e o GCHQ que procura aproveitar os conhecimentos e talentos existentes nas duas organizações para gerar os recursos, técnicas e *tradecraft* necessários;
- desenvolver a capacidade de uso de recursos cibernéticos ofensivos; e
- desenvolver a capacidade cibernética ofensiva de nossas Forças Armadas como parte integrante de suas operações, aumentando assim o impacto global da ação militar.

Avaliação dos resultados

6.5.4. O êxito do governo em desenvolver a capacidade cibernética ofensiva será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- o Reino Unido ser líder mundial em capacidade cibernética ofensiva; e
- o Reino Unido contar com um conjunto de competências e conhecimentos especializados, necessários para desenvolver e aplicar sua capacidade cibernética ofensiva soberana.

6.6. AUMENTO DA CAPACIDADE SOBERANA – CRIPTOGRAFIA

6.6.1. A criptografia é fundamental para a proteção de nossas informações mais sigilosas e para o planejamento das ações das Forças Armadas e do uso de nossos recursos de segurança nacional. Para manter essa capacidade, será necessário contar com conhecimentos e tecnologias do setor privado, assegurados por meio do GCHQ. É provável que isso envolva atividades no Reino Unido realizadas por cidadãos britânicos com a necessária habilitação de segurança, trabalhando em empresas privadas dispostas a atuar com total transparência para com o GCHQ no que se refere à concepção e implementação. O Ministério da Defesa e o GCHQ estão atualmente em processo de estudo do custo a longo prazo da manutenção desses recursos criptográficos soberanos, com base nas condições de mercado e em consulta com as empresas aptas a fornecer tais soluções.

Objetivo

6.6.2. Temos a confiança de que o Reino Unido sempre terá controle político dos recursos criptográficos vitais para sua segurança nacional e, portanto, contará com os meios necessários à proteção dos segredos nacionais.

Nossa abordagem

6.6.3. Serão adquiridos meios que permitam a comunicação com nossos aliados e garantam a disponibilidade de sistemas de informação, bem como de informações confiáveis nos momentos e locais oportunos. Em estreita colaboração com outras repartições e agências públicas, caberá ao GCHQ e ao Ministério da Defesa a definição conjunta de requisitos soberanos e da melhor forma de atender a esses requisitos nos casos em que os fornecedores sejam obrigatoriamente nacionais. Para isso, será criado um marco conjunto para a definição dos requisitos necessários para garantir a nossa vantagem operacional e liberdade de ação.

Avaliação dos resultados

6.6.4. O êxito do governo em manter sua capacidade criptográfica será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- a capacidade criptográfica soberana do Reino Unido ser eficaz em manter seus segredos e informações sigilosas a salvo da divulgação não autorizada.

CRIPTOGRAFIA

A criptografia é o processo de codificação de dados ou informações para impedir o acesso não autorizado.

O governo é a favor da criptografia como elemento fundamental para a solidez da economia da Internet, permitindo manter os dados pessoais e a propriedade intelectual seguros e garantindo a segurança do comércio online.

Contudo, com a evolução dos avanços tecnológicos, é preciso assegurar que não haja "espaços seguros" que permitam que terroristas e criminosos operem fora do alcance da lei.

Em parceria com o setor privado, o governo deve acompanhar a evolução tecnológica e assegurar, por meio de uma legislação robusta e uma fiscalização ostensiva, que as agências policiais e de inteligência possam acessar o conteúdo das comunicações entre terroristas e criminosos. A legislação existente permite que as comunicações de criminosos e terroristas sejam interceptadas mediante a obtenção de mandado. As empresas têm a obrigação de cumprir esses mandados, disponibilizando as comunicações solicitadas à autoridade competente. Mediante apresentação de mandado, as empresas devem remover qualquer criptografia aplicada por elas ou por sua conta, de modo que o material fornecido se torne legível. De acordo com a lei, as empresas são obrigadas a tomar medidas "razoáveis" para o cumprimento de mandados, sendo que em eventual avaliação de razoabilidade, serão analisadas, inclusive, as medidas tomadas pela empresa para a remoção de criptografia.

7. DESENVOLVER

7.0.1. O eixo DESENVOLVER desta estratégia define como o Reino Unido pretende adquirir e consolidar os recursos e estruturas necessárias para se proteger da ameaça cibernética.

7.0.2. O Reino Unido necessita de profissionais de segurança cibernética mais talentosos e qualificados.O governo pretende tomar medidas imediatas para preencher a crescente lacuna entre a procura e oferta de profissionais de segurança cibernética, trazendo novo fôlego para esta área de educação e ensino. Trata-se de um objetivo de transformação a longo prazo cuja consecução se iniciará no âmbito desta estratégia, mas que deve continuar além do horizonte de 2021. Uma mão de obra qualificada é a força vital de qualquer ecossistema de segurança cibernética que pretenda assumir uma posição de liderança mundial. Caberá a esse ecossistema assegurar que as *start-ups* cibernéticas tenham êxito no mercado e recebam os investimentos e o apoio necessários. Embora essa inovação e vigor econômico somente possam emanar do próprio setor privado, o governo atuará no apoio ao seu desenvolvimento e na promoção do setor de segurança cibernética junto ao mercado mundial. É necessário que exista um segmento de pesquisa científica dinâmica e pujante para viabilizar a formação de profissionais altamente qualificados e para que as novas ideias se traduzam em produtos de ponta.

7.1. FORTALECIMENTO DA CAPACITAÇÃO EM SEGURANÇA CIBERNÉTICA

7.1.1. O Reino Unido deve tratar das questões sistêmicas centrais do déficit de competências cibernéticas: a falta de jovens interessados em ingressar na profissão; a escassez de especialistas em segurança cibernética; a falta de exposição aos conceitos de segurança cibernética e da informação em cursos de computação; a falta de professores devidamente qualificados; e a falta de definição de rotas de formação e de carreira para a profissão.

7.1.2. Esse cenário exige uma rápida intervenção do governo para tratar da atual escassez e desenvolver uma estratégia coerente de longo prazo que, a partir dessas intervenções, contribua para sanar o déficit de competências. No entanto, há de se reconhecer que esse esforço, para que cause um impacto profundo, deverá ser colaborativo, contando com a contribuição de diversos atores e influenciadores nas administrações regionais, no setor público, nas instituições de ensino e acadêmicas e no setor privado.

Objetivo

7.1.3. É ambição do governo assegurar a formação interna dos melhores talentos em segurança cibernética, além de financiar intervenções específicas a curto prazo que contribuam para tratar do déficit de profissionais específicos. Também serão definidos e desenvolvidos os conhecimentos em segurança cibernética necessários para que toda a população e a mão de obra do país estejam aptos a exercer atividades online com segurança.

7.1.4. Para isso, serão necessárias ações nos próximos vinte anos, e não apenas nos próximos cinco. Será definido um conjunto de ações coordenadas e de longo prazo necessárias para que o governo, o setor privado, as instituições de ensino e o meio acadêmico possam garantir a formação permanente de profissionais de segurança cibernética competentes, que cumpram os padrões definidos e preencham as qualificações necessárias para exercer sua profissão com aptidão e segurança.

7.1.5. Também será tratado o déficit de qualificação na Defesa. Atuaremos para atrair para o serviço público especialistas cibernéticos que sejam altamente qualificados e aptos a manter a nossa segurança nacional. Seu rol de conhecimentos deve incluir a compreensão do impacto do ciberespaço nas operações militares.

Nossa abordagem

7.1.6. Será proposta e implementada uma estratégia autossustentável de capacitação que, a partir das iniciativas existentes, contribua para

integrar a segurança cibernética no sistema educacional. Com isso, será possível dar continuidade à evolução do ensino de informática e incorporar a segurança cibernética no currículo. Todo estudante de ciências da computação e tecnologias digitais deve aprender os fundamentos da segurança cibernética e poder trazer esses conhecimentos para o mercado de trabalho. No âmbito desses esforços, também será abordada a desigualdade de gênero nas profissões cibernéticas, assim como a necessidade de atrair profissionais de origens mais diversas, a fim de contribuir para uma maior diversificação do nosso banco de talentos. Atuaremos em estreita colaboração com as Administrações Regionais para promover uma abordagem harmonizada em todo o Reino Unido.

7.1.7. Serão definidas com maior clareza as atribuições e responsabilidades dos setores público e privado, e sua possível evolução no tempo. O governo do Reino Unido e as administrações regionais desempenham um importante papel na criação de um ambiente propício para a formação de competências em segurança cibernética e para atualização do sistema de ensino conforme a evolução das necessidades do governo e da iniciativa privada. Os empregadores também têm uma responsabilidade importante no sentido de definir claramente suas necessidades e capacitar e desenvolver seus colaboradores e os jovens recém ingressados na profissão. O setor privado tem um papel importante no desenvolvimento de rotas de formação e de carreira atraentes aos jovens, em parceria com universidades, entidades profissionais e entidades de classe.

7.1.8. Reconhecendo ser coletivo o desafio representado pelo déficit de competências, será criado um grupo consultivo de capacitação formado por representantes do governo, empregadores, entidades profissionais, instituições de ensino e meio acadêmico, fortalecendo a articulação entre estes setores-chave. Caberá ao grupo contribuir para a formulação de uma estratégia de longo prazo que acompanhe a evolução desse vasto domínio que são as ciências digitais, assegurando que as questões relativas à segurança cibernética estejam alinhadas e contempladas na estratégia. O grupo atuará de forma colaborativa com órgãos similares no Reino Unido.

7.1.9. Paralelamente a esse trabalho, o governo investirá em uma série de iniciativas que introduzam melhorias imediatas e tragam subsídios para a formulação da estratégia de capacitação de longo prazo. Dentre essas iniciativas, destacam-se:

- a criação de um programa voltado às escolas, visando promover uma transformação no ensino e na formação especializada em segurança cibernética para jovens talentos na faixa etária de 14 a 18 anos (envolvendo atividades em sala de aula, atividades após o período escolar com orientadores especialistas, projetos desafiadores e cursos de verão);
- criação de programas de aprendizagem de nível superior nos setores de energia, finanças e transportes, preenchendo as lacunas de competências existentes em áreas essenciais;
- criação de um fundo de reciclagem de profissionais já ingressados no mercado de trabalho e que demonstrem elevada aptidão para a profissão de segurança cibernética;
- identificação e apoio a cursos de graduação e pós-graduação em segurança cibernética, e identificação e preenchimento de lacunas de competências especializadas, reconhecendo o papel fundamental desempenhado pelas universidades na formação de profissionais;
- apoio à acreditação da formação de professores em segurança cibernética. Este trabalho servirá para capacitar professores e outros docentes em segurança cibernética, além de definir a metodologia de acreditação externa desses profissionais;
- desenvolvimento da profissão de segurança cibernética, revestindo-a do status de "*Royal Chartered*" até 2020 e formando um corpo de profissionais de excelência em segurança cibernética no setor, o qual servirá como referência para orientar, influenciar e subsidiar as políticas nacionais sobre o tema;
- criação de uma Academia de Defesa Cibernética como centro de excelência para formação e exercícios de segurança cibernética no Ministério da Defesa e no

setor público em geral, tratando das necessidades de formação especializada e de ensino em geral;
- desenvolvimento de oportunidades de colaboração nas áreas de formação e ensino entre governo, Forças Armadas, iniciativa privada e meio acadêmico, bem como estruturas para a manutenção e aplicação dos conhecimentos adquiridos; e
- atuação junto ao setor privado para expandir o programa *CyberFirst,* identificando e formando um banco diversificado de jovens talentos para defender a nossa segurança nacional; e
- inclusão da segurança cibernética e tecnologias digitais nos cursos relacionados oferecidos pelo sistema de ensino, desde o ensino primário até a pós-graduação, estabelecendo padrões de excelência, melhorando a qualidade e construindo uma base sólida para o avanço no tema.

Por ser o ensino um aspecto descentralizado no Reino Unido, algumas dessas iniciativas acontecerão predominantemente na Inglaterra. No entanto, atuaremos em colaboração com as Administrações Regionais para promover uma abordagem harmonizada nos sistemas de ensino do país.

Avaliação dos resultados

7.1.10. O êxito do governo em fortalecer a capacitação em segurança cibernética será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- existirem rotas efetivas e claras para o ingresso na profissão de segurança cibernética, que sejam atraentes para pessoas de diversas origens;
- até 2021, a segurança cibernética ser ensinada efetivamente como parte integrante dos cursos relacionados, desde o ensino primário até a pós-graduação;
- a segurança cibernética ser amplamente reconhecida como profissão estabelecida, com trajetórias de carreira bem definidas, e ser revestida do status de "*Royal Chartered*";
- integração de conhecimentos adequados em segurança cibernética no desenvolvimento contínuo de não profissionais de segurança cibernética, abrangendo todo o mercado de trabalho; e
- o Governo e as Forças Armadas terem acesso a especialistas cibernéticos capazes de preservar a segurança e a resiliência do Reino Unido.

7.2. ESTÍMULO AO CRESCIMENTO NO SETOR DE SEGURANÇA CIBERNÉTICA

7.2.1. Nossa moderna economia digital requer um setor de segurança cibernética inovador e pujante. As empresas de segurança cibernética do Reino Unido oferecem tecnologias líderes de mercado, além de serviços de formação e consultoria aos setores privado e público. Mas, por mais que Reino Unido detenha posição de liderança no setor, enfrenta uma concorrência feroz para permanecer à frente. Há também barreiras a serem superadas pelo governo. Ainda que as empresas e instituições de ensino e pesquisa do Reino Unido sejam capazes de desenvolver tecnologias de ponta, algumas necessitam de apoio para desenvolver os conhecimentos comerciais e empresariais necessários para obterem êxito no mercado. Existem lacunas de financiamento que impedem o crescimento e expansão de PMEs em novos mercados e territórios. Os produtos e serviços mais inovadores, capazes de contribuir para nos manter à frente das ameaças, enfrentam dificuldade em encontrar clientes dispostos a serem os primeiros a adotarem as soluções. Superar esses desafios exige que o governo, o setor privado e o meio acadêmico trabalhem juntos de forma efetiva.

Objetivo

7.2.2. O governo fomentará a criação de um setor de segurança cibernética inovador, próspero e em crescimento no Reino Unido, formando um ecossistema em que:

- as empresas de segurança possam ter êxito e obter os investimentos necessários para o seu crescimento;
- as melhores mentes do governo, do meio acadêmico e do setor privado possam atuar

de forma colaborativa para estimular a inovação; e
- os clientes do governo e do setor privado tenham a confiança e estejam preparados para adotar serviços de ponta.

Nossa abordagem

7.2.3. Para isso, pretende-se:

- comercializar a inovação no meio acadêmico, oferecendo capacitação e consultoria nesse sentido aos acadêmicos;
- criar dois centros de inovação que fomentem o desenvolvimento de produtos cibernéticos de ponta e a criação de novas e dinâmicas empresas de segurança cibernética, os quais formarão a base de um conjunto de iniciativas destinadas a dar às *start-ups* o apoio que necessitam para conquistar seus primeiros clientes e atrair novos investimentos;
- destinar parte dos £ 165 milhões do Fundo de Defesa e Inovação Cibernética (*Defence and Cyber Innovation Fund*) para financiar a contratação de produtos e serviços inovadores em defesa e segurança;
- disponibilizar instalações de teste onde as empresas possam desenvolver seus produtos, além de uma metodologia que agilize a avaliação da próxima geração de produtos e serviços de segurança cibernética, proporcionando ao consumidor maior confiança em seu uso;
- utilizar os conhecimentos coletivos adquiridos pela Parceria Público-Privada para o Crescimento Cibernético, a fim de orientar futuras intervenções de crescimento e inovação;
- auxiliar empresas de todos os portes em seus esforços de expansão e acesso aos mercados internacionais; e
- promover a adoção de normas internacionalmente aceitas que viabilizem o acesso ao mercado do Reino Unido.

7.2.4. O peso dos contratos públicos também será utilizado para estimular a inovação. O governo enfrenta alguns dos maiores desafios e maiores ameaças de segurança cibernética. Podemos, e devemos, buscar as soluções mais eficazes para sanar esses problemas. Para isso, é preciso facilitar os negócios entre empresas menores e a administração pública. É preciso também que o governo seja menos avesso ao risco de testar e utilizar novos produtos. Será uma solução vantajosa para ambas as partes: o governo,que poderá contar com os melhores serviços disponíveis no mercado, e as tecnologias inovadoras, que terão um cliente disposto a adotá-las antecipadamente, facilitando a captação de investimentos e a expansão da base de clientes. Todas as esferas do governo, inclusive as Administrações Regionais, serão incentivadas a adotar abordagens similares.

"Queremos criar um ecossistema cibernético propício à proliferação de *start-ups* cibernéticas e que permita que obtenham os investimentos e o apoio necessário para conquistar negócios mundo afora, além de formar um *pipeline* de inovação que canalize ideias entre o setor privado, o setor público e o meio acadêmico".

Matt Hancock,
Ministro de Estado da Cultura e Assuntos Digitais

Avaliação dos resultados

7.2.5. O êxito do governo em fomentar o crescimento do setor de segurança cibernética será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- crescimento anual acima da média do setor cibernético do Reino Unido;
- aumento significativo do investimento em empresas embrionárias;
- adoção pelo governo de tecnologias de segurança cibernética mais inovadoras e eficazes.

7.3. PROMOÇÃO DA CIÊNCIA E DA TECNOLOGIA DE SEGURANÇA CIBERNÉTICA

7.3.1. O forte setor de ciência e tecnologia do Reino Unido e suas pesquisas de ponta sustentam sua posição de liderança global em segurança cibernética. Para preservar e consolidar a reputação do Reino Unido como líder mundial em

pesquisa de ponta, nossas instituições de pesquisa devem continuar a atrair as mentes mais brilhantes no campo da segurança cibernética. Para isso, devem ser criados centros de excelência que atraiam os cientistas e pesquisadores mais capacitados e dinâmicos, e devem ser intensificadas as parcerias entre meio acadêmico, governo e setor privado. Nesse âmbito, o governo terá um papel de fomentador e articulador dessas colaborações. O sucesso nesses esforços se manifestará na criação de um ecossistema autossustentável que permita que as ideias, e as pessoas, circulem entre os três setores de forma mutuamente benéfica.

Objetivo

7.3.2. Até 2021, o Reino Unido consolidará sua posição como líder mundial em ciência e tecnologia cibernética. Através de parcerias flexíveis entre universidades e o setor privado, a produção científica será traduzida em produtos e serviços de sucesso comercial. O Reino Unido deve manter sua reputação de excelência em inovação, inclusive nas áreas que estão entre suas grandes vocações, como o setor financeiro.

Nossa abordagem

7.3.3. Para isso, o governo incentivará a colaboração, modelos inovadores e flexíveis para o financiamento de pesquisas, e a comercialização da produção científica. O governo fará com que os aspectos humanos e comportamentais do crime cibernético recebam a devida atenção e que não apenas os sistemas técnicos, como também os processos de negócios e estruturas organizacionais, sejam contemplados na ciência e tecnologia cibernética.

7.3.4. Essas ações contribuirão para a criação de produtos, sistemas e serviços que sejam "seguros por padrão", que contemplem os aspectos de segurança desde sua concepção, e que exijam a escolha deliberada do usuário de desabilitar os recursos de segurança.

7.3.5. Será publicada uma Estratégia de Ciência e Tecnologia Cibernética após ampla consulta junto a parceiros e outras partes interessadas. Nela serão identificadas as áreas de ciência e tecnologia que o governo, o setor privado e o meio acadêmico consideram importantes e as lacunas na atual capacidade tecnológica do país.

7.3.6. O governo continuará a oferecer financiamento e apoio aos Centros Acadêmicos de Excelência, instituições de pesquisa e Centros de Formação Doutoral. Também será criado um novo instituto de pesquisa em uma área de importância estratégica. Serão financiados, ainda, pesquisas em áreas onde sejam identificadas lacunas na Estratégia de Ciência e Tecnologia Cibernética a ser publicada. Dentre as principais áreas a serem consideradas, destacam-se: análise de *big data*; sistemas autônomos; sistemas de controle industrial de alta confiabilidade; sistemas ciberfísicos e a Internet das Coisas; cidades inteligentes; verificação automatizada de sistemas; e ciência da segurança cibernética.

7.3.7. O governo continuará a patrocinar estudantes de doutorado nos Centros Acadêmicos de Excelência, ampliando o número de britânicos com conhecimentos cibernéticos especializados.

7.3.8. Serão mantidas parcerias com órgãos como Innovate UK e com os Conselhos de Pesquisa, a fim de promover a colaboração entre setor privado, governo e meio acadêmico. Para subsidiar essas parcerias, serão analisadas as melhores práticas relacionadas a classificações de segurança e serão identificados especialistas com credenciamento de segurança, incluindo acadêmicos. Dessa forma, até mesmo os trabalhos que envolvam interação entre o espaço público e o sigiloso poderão ocorrer da forma mais colaborativa possível.

7.3.9. O governo lançará e financiará um "grande desafio" que consistirá em identificar e fornecer soluções inovadoras para alguns dos problemas mais urgentes na segurança cibernética. A *CyberInvest*, uma nova parceria público-privada de apoio à pesquisa em segurança cibernética de ponta e à proteção do Reino Unido no ciberespaço, fará parte da nossa estratégia na construção de parcerias entre o meio acadêmico, governo e iniciativa privada.

Avaliação dos resultados

7.3.10. O êxito do governo em promover a ciência e tecnologia em segurança cibernética será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- aumento significativo do número de empresas britânicas capazes de comercializar com êxito a produção científica cibernética, e redução das lacunas identificadas na capacidade de pesquisa em segurança cibernética do Reino Unido, através de medidas eficazes para preenchê-las; e
- o Reino Unido ser considerado um líder global em pesquisa e inovação em segurança cibernética.

7.4. MONITORAMENTO EFETIVO DO HORIZONTE

7.4.1. O Governo deve assegurar que os processos de decisão acompanhem a evolução cibernética, geopolítica e tecnológica. Para isso, é preciso fazer uso efetivo de um amplo processo de monitoramento e análise do horizonte. Precisamos investir na antecipação às futuras ameaças e às mudanças no mercado que possam afetar nossa resiliência cibernética nos próximos cinco a dez anos. Precisamos de programas de monitoramento de horizonte que gerem recomendações para subsidiar a política governamental atual e futura e o planejamento de nossos programas.

Objetivo

7.4.2. O governo assegurará que seja feita uma avaliação rigorosa do risco cibernético, e que essa avaliação seja integrada nas políticas de segurança cibernética e outras políticas tecnológicas, juntamente com análises de "todas as fontes" (*all-source*) e outras evidências disponíveis. Serão consolidadas as análises de horizonte da área de segurança nacional e de outras áreas para assegurar uma avaliação holística dos desafios e oportunidades emergentes.

Nossa abordagem

7.4.3. Nesse sentido, pretende-se:

- identificar lacunas nos trabalhos atuais e coordenar os trabalhos entre disciplinas a fim de desenvolver uma abordagem holística de monitoramento do horizonte da segurança cibernética;
- promover uma melhor integração dos aspectos técnicos da segurança cibernética com as ciências comportamentais;
- apoiar o monitoramento rigoroso do mercado do crime cibernético, visando identificar novas ferramentas e serviços que viabilizem a transferência tecnológica para estados hostis, terroristas ou criminosos;
- analisar tecnologias emergentes de controle de processos conectados à Internet;
- antecipar-se às vulnerabilidades associadas às moedas digitais; e
- monitorar as tendências do mercado relacionadas às tecnologias de telecomunicações, desenvolvendo defesas precoces contra futuros ataques previstos.

7.4.4. Reconhecemos que o monitoramento de horizonte ultrapassa o aspecto técnico, englobando também as dimensões política, econômica, legislativa, social e ambiental. A segurança cibernética é apenas um dos aspectos que um monitoramento de horizonte eficaz é capaz de abordar. Portanto, nas atividades de monitoramento de horizonte nessas outras áreas das políticas públicas, devem ser levadas em conta eventuais repercussões na segurança cibernética.

7.4.5. Também devemos assegurar que a formulação de políticas cibernéticas siga uma abordagem baseada em evidências, considerando as avaliações de todas as fontes disponíveis. Essas fontes podem incluir, por exemplo:

- evidências técnicas específicas, por exemplo, sobre a Internet das Coisas ou a futura participação de materiais avançados no mercado; e
- tendências estratégicas e sociais internacionais e seu impacto na esfera cibernética.

7.4.6. Devemos assegurar que a segurança cibernética seja contemplada no âmbito da Célula de Análise de Tecnologias e Inovações

Emergentes (*Emerging Technology and Innovation Analysis Cell – ETIAC*), órgão interministerial a ser criado para identificar ameaças e oportunidades tecnológicas relevantes para a segurança nacional, e que o espaço cibernético seja objeto das análises realizadas nas atuais estruturas de monitoramento de horizonte, inclusive nas análises do Government Futures Group (GFG) e do Grupo Consultivo da Secretaria do Gabinete para Monitoramento de Horizonte (*Cabinet Secretary's Advisory Group on horizon scanning – CSAG*).

Avaliação dos resultados

7.4.7. O êxito do governo em criar recursos eficazes de monitoramento de horizonte será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- integração de processos interministeriais de monitoramento de horizonte e de análise *all-source* na formulação de políticas cibernéticas; e
- o impacto da segurança cibernética ser considerado em todos os processos interministeriais de monitoramento de horizonte.

8. AÇÃO INTERNACIONAL

8.1. Nossa prosperidade econômica e bem-estar social dependem cada vez mais da abertura e segurança de redes que se estendem além das nossas fronteiras. É fundamental que trabalhemos em estreita colaboração com parceiros internacionais para assegurar a continuidade de um espaço cibernético livre, aberto, pacífico e seguro, e que continue a proporcionar esses benefícios. A tendência é que essas parcerias se tornem ainda mais importantes a partir da integração dos próximos bilhões de usuários na Internet.

8.2. A cooperação internacional em questões cibernéticas tornou-se uma parte fundamental do debate mundial sobre economia e segurança. Trata-se de uma área das políticas públicas que vive uma rápida evolução, sem que haja uma visão internacional unificada sobre o tema. O Reino Unido e seus aliados têm tido algum êxito na implantação de um sistema internacional regulamentado: houve consenso de que o direito internacional se aplica no espaço cibernético; que os direitos humanos também se aplicam no espaço cibernético da mesma forma que fora dele; e houve amplo consenso de que a abordagem multi-participada é a melhor forma de tratar das complexidades da governança da Internet. No entanto, com as crescentes divergências quanto à melhor forma de abordar o desafio de conciliar a segurança nacional com os direitos e liberdades individuais, o consenso mundial, se é que existe, permanece frágil.

"Devemos atuar em âmbito internacional para chegar a um consenso quanto às normas necessárias para garantir a futura segurança e prosperidade do Reino Unido no ciberespaço".

Boris Johnson,
Secretário de Relações Internacionais

Objetivos

8.3. O Reino Unido almeja preservar a longo prazo um espaço cibernético livre, aberto, pacífico e seguro, impulsionando o crescimento econômico e sustentando a segurança nacional do país. Nesse sentido, o Reino Unido continuará a: defender o modelo multi-participado de governança da Internet; opor-se à localização de dados; e atuar na capacitação de nossos parceiros para fortalecer sua segurança cibernética. Para reduzir as ameaças ao Reino Unido e aos nossos interesses, muitos dos quais têm origem no exterior, procuraremos influenciar os processos de decisão dos atores envolvidos em cibercriminalidade, espionagem cibernética e atividades cibernéticas destrutivas, e daremos continuidade à construção de estruturas de cooperação internacional.

Nossa abordagem

8.4. Para isso, pretende-se:

- fortalecer e adotar uma compreensão consensual daquilo que constitui comportamento responsável por parte dos Estados no espaço cibernético;
- consolidar o consenso de que o direito internacional se aplica no ciberespaço;
- continuar a promover a definição de normas voluntárias, não vinculativas, de comportamento responsável dos Estados;
- apoiar a propositura e implementação de medidas para fortalecer a confiança;
- ampliar a nossa capacidade de desarticular e levar os criminosos atuantes no exterior à justiça, principalmente em jurisdições que apresentam dificuldade de fiscalização;
- contribuir para a criação de um ambiente que permita que as nossas agências policiais trabalhem em conjunto para eliminar os espaços em que cibercriminosos possam agir impunes;
- promover a resiliência do espaço cibernético, influenciando as normas técnicas internacionais que regem as tecnologias emergentes (incluindo a criptografia), tornando o espaço cibernético mais seguro em sua concepção, e promovendo as melhores práticas adotadas no mercado;
- atuar para desenvolver abordagens comuns entre países que partilham da mesma visão em áreas como criptografia robusta, que têm implicações transfronteiriças;

- contribuir para a capacitação de terceiros para o enfrentamento das ameaças ao Reino Unido e aos nossos interesses no exterior;
- continuar a apoiar nossos parceiros no desenvolvimento de sua segurança cibernética: tendo em vista que dividimos o mesmo espaço cibernético, seremos coletivamente mais fortes se cada país reforçar suas defesas;
- garantir que a OTAN esteja preparada para os conflitos do século XXI, que terão como palco não apenas o campo de batalha, como também o espaço cibernético;
- atuar junto aos nossos aliados para assegurar que a atuação da OTAN seja tão eficaz no espaço cibernético quanto o é em terra, no ar e no mar; e
- garantir que o "*London Process*", uma série de conferências internacionais sobre o espaço cibernético, continue a promover um consenso internacional no sentido de um espaço cibernético livre, aberto, pacífico e seguro.

8.5. Existem diversas parcerias e instrumentos que continuarão a receber investimentos em prol da concretização dos nossos objetivos cibernéticos internacionais; não podemos alcançar nossos objetivos isoladamente. Essas ações compreendem:

- trabalhar com aliados tradicionais e novos parceiros para estabelecer e manter sólidas relações políticas e operacionais, estabelecendo condições políticas para a construção de fortes alianças globais;
- fazer valer a nossa influência junto a organizações multilaterais como as Nações Unidas, o G20, a União Europeia, a OTAN, a OSCE, o Conselho da Europa, a Commonwealth e a comunidade internacional; e
- estreitar as relações com atores não governamentais, ou seja, a iniciativa privada, sociedade civil, meio acadêmico e comunidade técnica. Esses atores são fundamentais para subsidiar o debate sobre a formulação de políticas internacionais e para fortalecer as mensagens políticas relacionadas às mais diversas questões cibernéticas. Nossos convênios acadêmicos propiciam uma plataforma neutra para a colaboração com parceiros internacionais.

Avaliação dos resultados

8.6 O êxito do governo em promover seus interesses internacionais em matéria de segurança cibernética será avaliado a partir dos avanços alcançados em busca dos seguintes resultados:

- fortalecimento da colaboração internacional, reduzindo as ameaças cibernéticas ao Reino Unido e aos seus interesses no exterior;
- definição consensual daquilo que constitui comportamento responsável por parte dos Estados no espaço cibernético;
- reforço da segurança cibernética dos nossos parceiros internacionais; e
- consolidação do consenso internacional quanto aos benefícios de um espaço cibernético livre, aberto, pacífico e seguro.

9. INDICADORES

9.1. A segurança cibernética continua a ser uma área de relativa baixa maturidade no que se refere à avaliação dos resultados e impactos por meio de indicadores. A ciência da segurança cibernética já é obscurecida pela hipérbole e pela ausência de dados calibrados. Esse fato é motivo de frustração tanto para os legisladores quanto para o setor privado, que se deparam, ambos, com dificuldades em auferir os resultados dos investimentos. O governo considera ser fundamental o uso eficaz de indicadores de desempenho para a concretização desta estratégia e para o direcionamento dos recursos a ela destinados.

9.2. Devemos assegurar que esta estratégia seja respaldada por um conjunto abrangente de indicadores que permitam medir o progresso em alcançar os resultados almejados. Além de representar um dos principais produtos desta estratégia, o NCSC terá um papel fundamental em viabilizar a consecução dos resultados previstos nesta estratégia por parte de outras esferas do governo, do setor privado e da sociedade.

9.3. O Anexo 3 apresenta uma correlação entre os indicadores de sucesso estabelecidos na estratégia e os resultados estratégicos almejados, indicadores estes que serão revistos anualmente para que reflitam adequadamente as metas e necessidades nacionais. Entre os principais resultados estratégicos, destacam-se os seguintes:

1. O Reino Unido ter a capacidade de detectar, investigar e combater as ameaças advindas das atividades cibernéticas de nossos adversários.

2. O impacto do crime cibernético no Reino Unido e nos seus interesses ser significativamente reduzido, e os criminosos cibernéticos serem dissuadidos de ter o Reino Unido como alvo.

3. O Reino Unido ter a capacidade de tratar e responder com eficácia a incidentes cibernéticos, reduzindo os prejuízos causados ao Reino Unido, e de combater seus adversários cibernéticos.

4. Nossas parcerias com o setor privado em matéria de defesa cibernética ativa contribuírem para tornar ineficazes os ataques de *phishing* e *malware* promovidos em grande escala.

5. O Reino Unido tornar-se um país mais seguro pela promoção de produtos e serviços de tecnologia que tenham a segurança integrada em sua concepção e habilitada por padrão.

6. As redes e serviços públicos terem máxima segurança desde sua implementação inicial. Os cidadãos poderem utilizar os serviços digitais do governo confiantes de que suas informações estão protegidas.

7. Todas as organizações no Reino Unido, independentemente de seu porte, adotarem uma gestão eficaz de riscos cibernéticos, tendo por base as diretrizes formuladas pelo NCSC e uma combinação equilibrada de regulamentação e incentivos.

8. Existir no Reino Unido um ecossistema propício para o desenvolvimento e manutenção de um setor de segurança cibernética capaz de atender às nossas demandas de segurança nacional.

9. O Reino Unido manter, de forma sustentável, uma safra permanente de profissionais cibernéticos formados internamente para atender às demandas crescentes de uma economia cada vez mais digital, tanto no setor público quanto no privado e na defesa.

10. O Reino Unido ser universalmente reconhecido como líder mundial em produção científica na área de segurança cibernética, apoiada por elevados níveis

de especialização no setor privado e no meio acadêmico.

11. O governo do Reino Unido planejar e se preparar para a adoção de políticas que se antecipem a futuras tecnologias e ameaças, tornando-se um país “à prova do futuro”.

12. As ameaças ao Reino Unido e aos seus interesses no exterior serem reduzidas graças à consolidação do consenso e da capacidade internacional de promover comportamentos responsáveis por parte dos Estados em um espaço cibernético livre, aberto, pacífico e seguro.

13. As políticas, organizações e estruturas do governo do Reino Unido serem simplificadas para garantir uma maior coerência e eficácia da resposta do país à ameaça cibernética.

9.4. Reconhecemos que algumas das nossas ambições para esta estratégia ultrapassam seu horizonte de cinco anos. Para que qualquer futuro investimento cibernético além de 2021 possa continuar a produzir o máximo efeito transformador, pretendemos que esses resultados de mais longo prazo, posteriores ao ano de 2021, sejam atribuídos ao setor privado, reguladores, auditores, seguradoras e outros atores dos setores público e privado, uma vez que a gestão eficaz dos riscos de segurança cibernética estará integrada nas atividades cotidianas de gestão de todos.

10. CONCLUSÃO: SEGURANÇA CIBERNÉTICA ALÉM DE 2021

10.1. A rápida evolução do meio cibernético trará constantemente novos desafios em função dos avanços tecnológicos e das tentativas de nossos adversários de explorá-los. Nesse contexto, esta estratégia visa assegurar a existência de um conjunto de políticas, instrumentos e recursos que garantam uma resposta rápida e flexível a cada novo desafio que surgir.

10.2. Se não agirmos com eficácia, a ameaça continuará à frente da nossa capacidade de proteção. Podemos esperar uma explosão de ameaças em todos os níveis.

10.3. Por outro lado, se tivermos êxito em concretizar as nossas ambições, todos os setores do governo, da iniciativa privada e da sociedade do Reino Unido cumprirão seu papel na proteção da segurança cibernética do país. Se conseguirmos incorporar a segurança "por padrão" na concepção das tecnologias oferecidas no mercado, os consumidores e as empresas terão menos motivos para se preocupar com a segurança cibernética. Se o Reino Unido for bem-sucedido em consolidar sua imagem como ambiente seguro para negócios online, será capaz de atrair um número maior de multinacionais e investidores para se instalarem no país. A segurança das redes das IEC e dos setores prioritários será mais eficaz. Por sua vez, os agressores que procurarem desenvolver ferramentas e técnicas de ataque contra os sistemas responsáveis por funções e dados críticos terão maior dificuldade em ultrapassar as diversas camadas de segurança que os cercam. Essas medidas tornarão menos vantajosa a relação de risco-recompensa para os cibercriminosos e atores mal-intencionados, que também passarão a estar sujeitos no exterior ao mesmo risco de ações penais a que está sujeito quem comete crimes tradicionais. Se conseguirmos integrar a segurança cibernética em todos os setores da sociedade, o governo poderá, então, se afastar de seu papel protagonista, permitindo que o mercado e a tecnologia assumam o processo de evolução da segurança cibernética em toda a economia e na sociedade.

10.4. Mesmo no cenário mais otimista, alguns dos desafios enfrentados pelo Reino Unido no domínio cibernético, seja pela sua dimensão ou por sua complexidade, podem exigir um prazo superior a cinco anos para serem superados. Contudo, esta estratégia estabelece os meios para transformar a nossa segurança no futuro e salvaguardar a nossa prosperidade na era digital.

ANEXO 1: SIGLAS

CCA– Centre for Cyber Assessment (Centro de Análise Cibernética). Vinculado ao NCSC, realiza análises de ameaças cibernéticas a serviço do governo britânico, dando subsídios à formulação de políticas.

CERT – Computer Emergency Response Team (Equipe de Resposta a Emergências Informáticas).

CERT-UK – Equipe de Resposta a Emergências Informáticas no Reino Unido.

CESG– Autoridade técnica nacional para asseguração de informações no Reino Unido. Oferece um serviço especializado, independente, de pesquisa e inteligência em segurança da informação para o governo do Reino Unido.

IEC– Infraestrutura Crítica. Elementos críticos da infraestrutura (ativos, instalações, sistemas, redes ou processos e os trabalhadores essenciais responsáveis por sua operação ou manutenção) cuja perda ou comprometimento possa causar:

a. grandes impactos prejudiciais à disponibilidade, à integridade ou ao fornecimento de serviços essenciais, incluindo serviços cuja integridade, se comprometida, possa resultar em fatalidades ou acidentes de grande proporção – considerando os impactos econômicos ou sociais significativos; e/ou

b. impactos significativos na segurança nacional, na defesa nacional ou no funcionamento do Estado.

CPNI – Centre for the Protection of National Infrastructure (Centro para a Proteção das Infraestruturas Nacionais). Propõe diretrizes que visam reduzir a vulnerabilidade das organizações inseridas na infraestrutura nacional ao terrorismo e à espionagem. Também atua em parceria com o NCSC para estabelecer orientações sobre a proteção holística contra ameaças do ciberespaço.

O CPNI mantém parcerias sólidas com organizações do setor privado inseridas na infraestrutura nacional, criando um ambiente de confiança onde possa haver um intercâmbio de informações em benefício de todos. As relações diretas são ampliadas por uma rede estendida que abrange outras repartições públicas e organizações de serviços profissionais.

DDoS – *Distributed Denial of Service* (Ataque Distribuído de Negação de Serviço). Inundação de um sistema de informação com um número de solicitações superior ao que é capaz de suportar, impedindo o acesso de usuários autorizados.

GCHQ – Government Communications Headquarters; centro para atividades de inteligência de sinais do governo e autoridade técnica cibernética nacional (*Cyber National Technical Authority – NTA*).

TIC – Tecnologias da Informação e das Comunicações.

MD – Ministério da Defesa

OTAN – Organização do Tratado do Atlântico Norte.

NCA – Agência Nacional de Combate ao Crime (National Crime Agency); departamento governamental não ministerial.

NCSC– National Cyber Security Centre.

OSCE– Organização para a Segurança e a Cooperação na Europa.

PME – Pequenas e médias empresas.

ANEXO 2: GLOSSÁRIO

Action Fraud – centro nacional para a comunicação de crimes de fraude e cibernéticos, que atua como ponto central de contato para a população e a iniciativa privada.

Defesa Cibernética Ativa (*Active Cyber Defense – ACD*) – consiste em adotar medidas de segurança proativas capazes de fortalecer a segurança de uma rede ou sistema e torná-lo mais robusto contra ataques.

Anonimização– uso de recursos criptográficos para ocultar ou mascarar a identidade na Internet.

Autenticação – processo de verificação da identidade ou outros atributos de um usuário, processo ou dispositivo.

Verificação automatizada de sistemas – medidas para garantir que os *softwares* e *hardware*s estejam funcionando como esperado e sem erros.

Sistema Autônomo – conjunto de redes de IP cujo roteamento está sob o controle de uma entidade ou domínio específico.

Big data – conjuntos de dados cujo grande volume impossibilita seu processamento e gerenciamento em tempo hábil com uso de *softwares* comerciais, e que requerem uma capacidade específica de processamento para suportar seu volume, velocidade de geração e multiplicidade de fontes.

Bitcoin – moeda e sistema de pagamento digitais.

Malware commodity – *malware* amplamente disponível para compra ou download gratuito e que não sofreu customização, sendo empregado por uma grande diversidade de atores maliciosos.

Exploração de Redes de Computadores (*Computer Network Exploitation – CNE*) – espionagem cibernética; uso de uma rede de computadores para infiltrar a rede de computadores-alvo e reunir informações de inteligência.

Mercado do Crime Cibernético – totalidade dos produtos e serviços que formam a base do ecossistema do crime cibernético.

Criptografia – ciência ou conjunto de técnicas utilizadas para analisar e decifrar códigos e cifras; criptoanálise.

Ataque cibernético – exploração deliberada de sistemas informáticos, empresas e redes dependentes da tecnologia com o intuito de causar danos.

Crimes cibernéticos – crimes ciberdependentes (aqueles que somente podem ser cometidos com recurso às Tecnologias da Informação e Comunicação (TIC), sendo estas ao mesmo tempo o instrumento e o alvo do crime); ou crimes ciberfacilitados (crimes que podem ser cometidos sem recurso às TIC, como fraude financeira, mas cuja escala e alcance são significativamente ampliadas pelo uso das TIC).

Ecossistema cibernético – conjunto interligado de infraestruturas, pessoas, processos, dados e tecnologias de informação e da comunicação, juntamente com o ambiente e as condições que influenciam essas interações.

Incidente cibernético – ocorrência que representa, ou possa representar, uma ameaça a um computador, dispositivo conectado à Internet ou rede, ou aos dados processados, armazenados ou transmitidos nesses sistemas, e que possa exigir uma ação de resposta para mitigar as consequências.

CyberInvest – programa público-privado, com orçamento de £ 6,5 milhões, destinado a fomentar a pesquisa em segurança cibernética de ponta e contribuir para a proteção do Reino Unido no ciberespaço.

Sistema ciberfísico – sistema com componentes computacionais e físicos integrados; sistema "inteligente".

Resiliência cibernética – capacidade geral dos sistemas e organizações de resistir a eventos cibernéticos e recuperar-se de eventuais danos causados.

Segurança cibernética – proteção aos sistemas interligados (*hardwares*, *softwares* e infraestruturas associadas), aos dados neles contidos e aos serviços que disponibilizam, contra o acesso não autorizado, prejuízos ou uso indevido. Isso inclui prejuízos causados pelo operador do sistema, seja intencional ou acidentalmente, ao não seguir os procedimentos de segurança ou ao ser manipulado para provocar tais prejuízos.

Desafio de Segurança Cibernética – competição que incentiva interessados a testar suas habilidades e a se interessar pela carreira de segurança cibernética.

Espaço cibernético – a rede interdependente de infraestruturas de tecnologia da informação, que inclui a Internet, as redes de telecomunicações, os sistemas informáticos, dispositivos ligados à Internet e os processadores e controladores incorporados. Pode se referir também ao mundo ou domínio virtual enquanto experiência ou conceito abstrato.

Ameaça cibernética – qualquer fato capaz de comprometer a segurança ou causar prejuízos aos sistemas de informação e aos dispositivos ligados à Internet (incluindo *hardwares*, *softwares* e infraestruturas associadas), aos dados neles contidos e aos serviços que disponibilizam, principalmente por meios cibernéticos.

Violação de dados – movimentação ou divulgação não autorizada das informações que circulam em uma rede para um terceiro não autorizado a acessar ou visualizar essas informações.

Domínio – o nome de domínio indica a localização de uma organização ou outra entidade na Internet e corresponde a um endereço IP (*Internet Protocol*).

Domain Name System (DNS) – sistema de nomeação para computadores e serviços de rede com base em uma hierarquia de domínios.

Doxing– prática de pesquisar, ou *hackear*, as informações cadastrais da vítima na Internet, para então publicá-las.

E-commerce – comércio eletrônico. Comércio realizado ou facilitado pela Internet.

Criptografar – transformar criptograficamente os dados (chamados de "texto simples") em "texto cifrado" para ocultar o significado original dos dados, evitando que sejam conhecidos ou utilizados.

Monitoramento de horizonte – análise sistemática de informações para identificar possíveis ameaças, riscos, questões e oportunidades emergentes, permitindo uma melhor preparação e a inclusão de ações de mitigação e exploração no processo de formulação de políticas.

Tratamento de incidentes – gerenciamento e coordenação das atividades de investigação e tratamento da ocorrência, ou possível ocorrência, de um evento cibernético adverso que possa comprometer ou causar danos a um sistema ou uma rede.

Resposta a incidentes – atividades que tratam dos efeitos diretos de curto prazo de um incidente, podendo também contribuir para a recuperação no curto prazo.

Sistema de Controle Industrial (*Industrial Control System – ICS*) – sistema de informação empregado no controle de processos industriais como manufatura, movimentação de produtos, produção e distribuição, ou no controle de ativos de infraestrutura.

Internet das Coisas Industrial (*Industrial Internet of Things – IIoT*) – aplicação do conceito de Internet das Coisas às tecnologias de manufatura e industriais.

Insider– pessoa com acesso autorizado aos dados e sistemas de informação de uma organização e

que pode representar uma ameaça cibernética, seja intencional, acidental ou inconscientemente.

Integridade – qualidade das informações precisas e completas e que não tenham sido alteradas acidental ou deliberadamente.

Internet – rede mundial de computadores que oferece diversas facilidades de informação e de comunicação, constituída de redes interligadas que utilizam protocolos de comunicação padronizados.

Internet das Coisas – totalidade dos dispositivos, veículos, edifícios e outros elementos dotados de sistemas eletrônicos, *softwares* e sensores que se comunicam e intercambiam dados pela Internet.

London Process – conjunto de medidas resultantes da Conferência de Londres sobre o Ciberespaço em 2011.

Malware – *software* ou código malicioso. Os *malwares* incluem vírus, *worms*, *trojans* e *spywares*.

Rede (de computadores) – conjunto de computadores hospedeiros (*host*) juntamente com as sub-redes ou inter-redes através das quais se comunicam.

Capacidade ofensiva cibernética – emprego de recursos cibernéticos para obstruir, negar, degradar ou destruir redes de computadores e dispositivos conectados à Internet.

Patch – é o processo de atualização de *softwares* para corrigir *bugs* e vulnerabilidades

Testes de penetração – atividades destinadas a testar a resiliência de uma rede ou instalação contra *hackers*, atividades estas que são autorizadas ou patrocinadas pela organização a ser submetida aos testes.

Phishing – uso de e-mails que aparentam ser de um remetente confiável para induzir os destinatários a clicar em links maliciosos ou anexos contaminados com *malwares*, ou a compartilhar informações sigilosas com terceiros desconhecidos.

Ransomware – *software* malicioso que impede o acesso do usuário a seus arquivos, computador ou dispositivo até que pague um resgate.

Reconhecimento – fase de um ataque em que o invasor reúne informações e mapeia as redes, além de testá-las para identificar vulnerabilidades que possam ser exploradas e *hackeadas*.

Risco – possibilidade de que determinada ameaça cibernética explore as vulnerabilidades de um sistema de informação, causando prejuízos.

Roteador – dispositivo responsável pela interconexão de redes lógicas e encaminhamento de informações para outras redes com base em endereços IP.

Script kiddie – indivíduo com poucos conhecimentos que utiliza *scripts* ou programas prontos, encontrados na Internet, para realizar ataques cibernéticos, como *defacements.*

Segurança por padrão – meios para possibilitar o uso seguro de tecnologias comerciais, em que a segurança é garantida por padrão para o usuário.

Segurança na concepção (*Secure by design*) – refere-se a *softwares*, *hardwares* e sistemas projetados desde sua concepção para oferecerem segurança.

***Spoofing* de SMS** – técnica que permite mascarar a origem de uma mensagem de texto SMS, substituindo o número de origem *(Sender ID*) por um texto alfanumérico. Pode serutilizada legitimamente por um remetente para substituir seu número de celular por seu próprio nome, ou pelo nome de sua empresa, por exemplo. Pode também ser empregada de forma ilegítima, por exemplo, para representar fraudulentamente um terceiro.

Engenharia social – técnicas utilizadas por invasores para enganar e manipular as vítimas, induzindo-as a executar uma ação ou revelar informações confidenciais.
Essas ações geralmente consistem na abertura de uma página Web maliciosa ou de um anexo indesejado.

Trusted Platform Module (TPM) – padrão internacional para criptoprocessadores seguros: microprocessadores dedicados destinados a proteger os *hardwares* pela integração de chaves criptográficas nos dispositivos.

Usuário – pessoa, entidade organizacional ou processo automatizado que acessa um sistema, estando autorizado ou não.

Vírus – programa malicioso capaz de se espalhar para outros arquivos.

Vishing – *vishing*, ou *phishing* de voz, refere-se ao uso da tecnologia de voz (telefones fixos, telefones celulares, e-mail de voz, etc.) para induzir as vítimas a revelar informações financeiras ou pessoais sigilosas para entidades não autorizadas, geralmente com o intuito de promover um golpe.

Vulnerabilidades – *bugs* em programas de *software* que possam ser explorados por invasores.

ANEXO 3: SÍNTESE DO PROGRAMA DE IMPLEMENTAÇÃO

ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA 2016-2021

Visão: que o Reino Unido seja um país seguro e resiliente às ameaças cibernéticas, próspero e confiante no mundo digital.

Resultados estratégicos	Indicadores de sucesso (até 2021)	Contribui para
1. O Reino Unido ter a capacidade de detectar, investigar e combater, com eficácia, as ameaças advindas das atividades cibernéticas de nossos adversários.	• Consolidação de redes de intercâmbio de informações com nossos parceiros internacionais e acordos multilaterais ampliados para a promoção de condutas lícitas e responsáveis por parte dos Estados, contribuindo substancialmente para a nossa capacidade de entender e responder às ameaças e fortalecendo as defesas do Reino Unido. • Existência de medidas de defesa e dissuasão aliadas a estratégias específicas por país, tornando o Reino Unido um alvo mais difícil de ser atingido por atores estrangeiros hostis e terroristas cibernéticos. • Maior conhecimento da ameaça cibernética representada por atores estrangeiros hostis e terroristas, através da identificação e investigação de ameaças de terrorismo cibernético ao Reino Unido. • Garantia de que a capacidade técnica cibernética das organizações terroristas continue limitada, através da vigilância e desarticulação precoce das estruturas e atividades cibernéticas de terroristas, impedindo a evolução da sua capacidade. • O Reino Unido ser líder mundial em capacidade cibernética ofensiva. • O Reino Unido contar com um conjunto de competências e conhecimentos especializados, necessárias para desenvolver e aplicar sua capacidade cibernética ofensiva soberana. • A capacidade criptográfica soberana do Reino Unido ser eficaz em manter seus segredos e informações confidenciais a salvo da divulgação não autorizada.	DISSUADIR
2. O impacto do crime cibernético no Reino Unido e nos seus interesses ser significativamente reduzido, e os criminosos cibernéticos serem dissuadidos de ter o Reino Unido como alvo.	• Maior capacidade de desarticulação dos criminosos cibernéticos que promovam ataques ao Reino Unido, evidenciada pelo aumento das prisões e condenações e por um número maior de redes criminosas desarticuladas como consequência das intervenções dos órgãos policiais. • Maior capacidade de fiscalização, com aumento da capacidade e das competências tanto dos órgãos policiais especializados quanto dos convencionais, e uma maior capacidade de fiscalização no exterior; • Aumento da eficácia e da extensão das medidas de intervenção precoce (“PREVENIR”), dissuadindo e reabilitando possíveis infratores. • Redução das infrações cibernéticas de baixa complexidade pela dificultação do acesso e menor eficácia dos serviços criminosos cibernéticos.	DISSUADIR
3. O Reino Unido ter a capacidade de tratar e responder com eficácia a incidentes cibernéticos, reduzindo os prejuízos	• Uma maior proporção dos incidentes ser comunicada às autoridades, levando a uma melhor compreensão da dimensão e escala das ameaças. • Tratamento mais eficaz, eficiente e abrangente dos incidentes cibernéticos, fruto da criação do Centro Nacional de Segurança Cibernética (NCSC) como mecanismo centralizado de notificação e	DEFENDER

causados ao Reino Unido, e de combater seus adversários cibernéticos.	resposta a incidentes. • Abordarmos as causas-raiz dos ataques a nível nacional, reduzindo a ocorrência de ataques repetidos às mesmas vítimas e setores.	
4. Nossas parcerias com o setor privado em matéria de defesa cibernética ativa contribuírem para tornar ineficazes os ataques de phishing e malware promovidos em grande escala.	• Dificultação de ações de "*phishing*" por meio de defesas em grande escala contra a utilização de domínios maliciosos e uma proteção *antiphishing* mais ativa, e dificultação do uso de outras formas de comunicação, como "*vishing*" e *spoofing* de SMS, em ataques de engenharia social; • Bloqueio de uma proporção muito maior das comunicações de *malwares* e artefatos técnicos associados a ataques e exploração cibernética. • O tráfego de Internet e de telecomunicações no Reino Unido ser significativamente menos vulnerável a reencaminhamento por atores maliciosos. • Fortalecimento expressivo da capacidade de resposta do GCHQ, das Forças Armadas e da NCA diante de graves ameaças patrocinadas por Estados e criminosos.	DEFENDER
5. O Reino Unido tornar-se um país mais seguro pela promoção de produtos e serviços de tecnologia que tenham a segurança integrada em sua concepção e habilitada por padrão.	• A maioria dos produtos e serviços comerciais disponíveis no Reino Unido em 2021 contribuir para tornar o país mais seguro por possuir recursos de segurança habilitados por padrão ou integrados em sua concepção. • Os serviços públicos contarem com a confiança da população por serem implementados com o maior grau de segurança possível e por estarem os níveis de fraude dentro de parâmetros de risco aceitáveis.	DEFENDER
6. As redes e serviços públicos terem máxima segurança desde sua implementação inicial. Os cidadãos poderem utilizar os serviços digitais do governo confiantes de que suas informações estão protegidas.	• O governo conhecer profundamente o nível de risco à segurança cibernética em todo o governo e no setor público em geral. • Todas as repartições públicas e outros órgãos protegerem-se proporcionalmente ao seu nível de risco e segundo um padrão mínimo definido para o setor público. • As diversas repartições da administração pública e o setor público em geral serem resilientes e capazes de responder com eficácia a incidentes cibernéticos, mantendo suas funções e se recuperando com rapidez. • As novas tecnologias e serviços digitais implantados pelo governo terem segurança cibernética integrada por padrão. • O governo ter conhecimento e mitigar ativamente todas as vulnerabilidades conhecidas da Internet nos sistemas e serviços públicos. • Todos os fornecedores do governo atenderem às normas de segurança cibernética definidas.	DEFENDER
7. Todas as organizações no Reino Unido, independente de seu porte, adotarem uma gestão eficaz de riscos cibernéticos, tendo por base as diretrizes formuladas pelo NCSC e uma combinação equilibrada de regulamentação e incentivos.	• O governo conhecer o nível de segurança cibernética nas IEC e adotar medidas para intervir, quando necessário, para promover melhorias de interesse nacional. • Nossas empresas e organizações mais importantes estarem conscientizadas quanto ao nível da ameaça e adotarem práticas proporcionais de segurança cibernética. • O nível de segurança cibernética da economia britânica ser igual ou superior ao das economias avançadas comparáveis. • O número, a gravidade e o impacto dos ataques cibernéticos bem-sucedidos contra empresas no Reino Unido se reduzir como consequência da aplicação de normas de higiene cibernética. • Serem registradas melhorias na cultura de segurança cibernética no Reino Unido, fruto da maior conscientização das organizações e da população sobre os níveis de risco cibernético e as medidas de higiene cibernética que devem tomar para geri-los.	DEFENDER
8. Existir no Reino Unido um ecossistema propício para o	• Crescimento anual acima da média do setor cibernético do Reino Unido; • Aumento significativo do investimento em empresas	DESENVOLVER

desenvolvimento e manutenção de um setor de segurança cibernética capaz de atender às nossas demandas de segurança nacional.	embrionárias;	
9. O Reino Unido manter, de forma sustentável, uma safra permanente de profissionais cibernéticos formados internamente para atender às demandas crescentes de uma economia cada vez mais digital, tanto no setor público quanto no privado e na defesa.	• Existirem rotas efetivas e claras para o ingresso na profissão de segurança cibernética, que sejam atraentes para pessoas de diversas origens. • Até 2021, a segurança cibernética ser ensinada efetivamente como parte integrante dos cursos relacionados no sistema de ensino, desde o ensino primário até a pós-graduação; • A segurança cibernética ser amplamente reconhecida como profissão estabelecida, com trajetórias de carreira bem definidas, e ser revestida do status de "*Royal Chartered*". • Integração de conhecimentos adequados em segurança cibernética no desenvolvimento contínuo de não profissionais de segurança cibernética, em todo o mercado de trabalho. • O governo e as forças armadas terem acesso a especialistas cibernéticos capazes de preservar a segurança e a resiliência do Reino Unido.	DESENVOLVER
10. O Reino Unido ser universalmente reconhecido como líder mundial em produção científica na área de segurança cibernética, apoiada por elevados níveis de especialização no setor privado e no meio acadêmico.	• Aumento significativo do número de empresas britânicas capazes de comercializar com êxito as pesquisas científicas cibernéticas. Redução das lacunas identificadas na capacidade de pesquisa em segurança cibernética do Reino Unido, havendo medidas eficazes para preenchê-las. • O Reino Unido ser considerado um líder global em pesquisa e inovação em segurança cibernética.	DESENVOLVER
11. O governo do Reino Unido planejar e se preparar para a adoção de políticas que se antecipem a futuras tecnologias e ameaças, tornando-se um país "à prova do futuro".	• Integração de processos interministeriais de monitoramento de horizonte e de análise *all-source* na formulação de políticas cibernéticas. • O impacto da segurança cibernética ser considerado em todos os processos interministeriais de monitoramento de horizonte.	DESENVOLVER
12. As ameaças ao Reino Unido e aos seus interesses no exterior serem reduzidas graças à consolidação do consenso e da capacidade internacional de promover comportamentos responsáveis por parte dos Estados em um espaço cibernético livre, aberto, pacífico e seguro.	• Fortalecimento da colaboração internacional, reduzindo as ameaças cibernéticas ao Reino Unido e aos seus interesses no exterior; • Definição consensual daquilo que constitui comportamento responsável por parte dos Estados no espaço cibernético; • Reforço da segurança cibernética dos nossos parceiros internacionais; e • Consolidação do consenso internacional quanto aos benefícios de um espaço cibernético livre, aberto, pacífico e seguro.	AÇÃO E INFLUÊNCIA INTERNACIONAL
13. As políticas, organizações e estruturas do governo do Reino Unido serem	• As responsabilidades do governo em matéria de segurança cibernética serem compreendidas e seus serviços serem acessíveis. • Nossos parceiros conhecerem as melhores formas de interação	TRANSVERSAL

simplificadas para garantir uma maior coerência e eficácia da resposta do país à ameaça cibernética.	com o governo em assuntos de segurança cibernética	