

GUERRA CIBERNÉTICA

(Origem: Wikipédia)

A **ciberguerra** ou **guerra cibernética** é uma modalidade de [guerra](#) onde a conflitualidade não ocorre com armas físicas, mas através da confrontação com meios electrónicos e informáticos no chamado [ciberespaço](#). No seu uso mais comum e livre, o termo é usado para designar ataques, represálias ou intrusão ilícita num computador ou numa [rede](#). No entanto, uma genuína ciberguerra, situação que, em total rigor, até agora nunca ocorreu, implica, de um ponto de vista legal, o enquadramento da conflitualidade no âmbito do Direito dos Conflitos Armados ou [Direito Internacional Humanitário](#).¹⁴ Tais situações poderão surgir ligadas a conflitos políticos, económicos ou militares no mundo real, ou seja, ocorrer ao mesmo tempo de uma conflitualidade física, ou de forma totalmente autónoma. Por outro lado, estas ações poderão ter origem diretamente em estados, ou, então, ser protagonizadas por atores não estaduais atuando de forma autónoma. A possibilidade de ciberguerra resulta da existência de redes de computadores essenciais para o funcionamento de um país. Potenciais alvos são as infraestruturas críticas, nomeadamente as redes de energia elétrica, de gás e de água, os serviços de transportes, os serviços de saúde e financeiros.¹⁵

Pelas suas possíveis consequências económicas^{16 17 18} e danos que podem provocar ao normal funcionamento de um país, os ciberataques são motivo de crescente preocupação a nível internacional. Existem exemplos concretos do que poderão ser essas situações. Os ciberataques sofridos pela Estónia em 2007, mostraram como uma economia e serviços públicos da era digital podem sofrer graves anomalias de funcionamento ou até ficarem temporariamente indisponíveis.¹⁹ Por sua vez, na [Guerra na Ossétia do Sul em 2008](#), que opôs a [Geórgia](#) às forças separatistas ossetas apoiadas pela [Rússia](#), paralelamente às ações militares no terreno, os [sites](#) governamentais da Geórgia e de várias empresas públicas e privadas foram também alvo de ciberataques ²⁰, abrindo-se um novo campo de batalha no conflito. Num outro plano, os danos sofridos pelo [programa nuclear iraniano](#) tornados públicos em 2010, devido ao vírus [Stuxnet](#), evidenciaram as múltiplas potencialidades de uso de ciberarmas para os meios militares e de segurança. Naturalmente que as maiores e mais sofisticadas economias têm uma particular preocupação com este assunto, devido à crescente dependência da sua prosperidade face à tecnologia digital e às redes informáticas. Todavia, as ações para prevenir e punir ciberataques estão longe de obter consenso internacional. Isto ocorre não só pela complexidade técnica e jurídica das questões levantadas, como porque o uso de ciberarmas pode ser uma opção interessante, de guerra assimétrica, para vários países.

Infraestruturas críticas como alvo

A empresa de segurança norte-americana, McAfee, no seu relatório de 2010 intitulado "Sob Fogo Cruzado. Infraestrutura Crítica na Era da Guerra [Cibernética](#)",²¹ fez uma avaliação global das ameaças que impendem sobre as infraestruturas críticas – redes elétricas, de gás e de água, telecomunicações, transportes, serviços financeiros e de saúde, etc. O relatório baseou-se nos resultados de um inquérito efetuado a seiscentos executivos de [Tecnologia da Informação](#) (TI) responsáveis pela segurança em empresas de infraestruturas críticas de sete setores e catorze países. Estes responderam anonimamente a uma série de perguntas detalhadas sobre suas experiências com ciberataques e práticas de segurança.






As respostas evidenciaram que as redes e sistemas de controle de infraestruturas críticas estão constantemente sob o efeito de ciberataques. Frequentemente enfrentam também adversários de alto nível, existindo, em vários casos, suspeitas de envolvimento, não assumido, de países estrangeiros nos mesmos. O tipo de ciberataque também varia, desde o [ataque de negação de serviço](#) (DoS na sigla em língua inglesa), perpetrado em massa e concebido para derrubar sistemas de informação, até iniciativas subreptícias de penetração nas redes, com o objetivo de [espionagem](#). Um outro tipo de ataque consiste na introdução de um [software](#) malicioso na infraestrutura crítica. O [Stuxnet](#), considerado o mais poderoso vírus até agora criado.²² reflete essa possibilidade. Comprovou, num caso concreto – o [programa nuclear iraniano](#) – , como uma infraestrutura crítica de produção de energia pode ser alvo de um novo tipo de ato de ciberguerra, mostrando inovadoras possibilidades estratégicas para o atacante.²³ É consensual, entre os especialistas, o [Stuxnet](#) não poder ter sido produzido por um usuário doméstico até porque eram necessárias informações privilegiadas sobre o funcionamento das instalações nucleares iranianas, o que escapa, certamente, às possibilidades de hackers atuando isoladamente.

O impacto dos ciberataques também é bastante variável, mas algumas das consequências relatadas mostraram impactos negativos significativos. O custo reportado das paralisações decorrentes de grandes ataques excedeu US\$ 6 milhões por dia. Fora esse custo, a perda mais amplamente temida com os ciberataques é o dano à reputação, seguido pela perda de informações pessoais dos clientes.²⁴ Em termos de identificação e responsabilização dos autores, há problemas técnicos e jurídicos delicados e difíceis de ultrapassar. Desde logo, porque as instruções de um ciberataque, que são transmitidas para as redes, costumam vir de outros computadores infectados, usualmente pertencentes a terceiros inocentes. Quanto aos verdadeiros autores do ciberataque, normalmente ficam ocultos por detrás de barreiras e falsos vestígios. Esses fatores tornam difícil o rastreamento da sua verdadeira origem e limitam a possibilidade de punição legal pela incerteza quanto à autoria.

Assim, para os autores do relatório, o [ciberespaço](#) de hoje “lembra muito o que [Hobbes](#) chamou de um estado de natureza – uma ‘guerra de cada homem contra cada homem’. [Hobbes](#) imaginava que apenas o governo e a lei poderiam por fim a essa guerra”.²¹ Todavia, em matéria de proteção e segurança das infraestruturas críticas o papel dos governos torna-se complicado quando a maioria das infraestruturas críticas está nas mãos de empresas privadas. O problema tende ainda a ser mais complexo, e a vulnerabilidade potencialmente maior, quando as infraestruturas críticas nacionais são detidas numa percentagem significativa por capitais estrangeiros.

Cibercapacidades ofensivas e defensivas

Uma análise das capacidades ofensivas e defensivas de algumas das principais potências militares mundiais foi efetuada recentemente pelos norte-americanos, Richard Clarke e Robert Knake.²⁴ Colocaram um especial ênfase no aspecto das capacidades defensivas e das vulnerabilidades, considerando que estas facetas estavam a ser subavaliados pelo governo dos EUA. Segundo Clarke e Knake,²⁵ uma avaliação dessas capacidades deve ter em conta três dimensões: a) a capacidade ciberofensiva, entendida como a capacidade de efetuar ciberataques a outros Estados; b) a capacidade ciberdefensiva configurada como “a medida da capacidade de adoptar ações sob um ataque” ações essas que “irão bloquear ou mitigar esse ataque”; c) a ciberdependência medida como “a extensão em que um Estado está ligado e assente sobre redes e sistemas que podem ser vulneráveis no caso de um ciberataque. Adoptando estas três dimensões chegaram ao quadro estimativo dessas capacidades, apresentado em baixo.²⁶

Estados	Ciberataque	Ciberdefesa	Ciberdependência	Total
 Estados Unidos	8 pontos	1 ponto	2 pontos	11 pontos
 Rússia	7 pontos	4 pontos	5 pontos	16 pontos
 China	5 pontos	6 pontos	4 pontos	15 pontos
 Irão	4 pontos	3 pontos	5 pontos	12 pontos
 Coreia do Norte	2 pontos	7 pontos	9 pontos	18 pontos

Clarke e Knake justificam esta hierarquização de cibercapacidades afirmando que “a China tem uma elevada pontuação na defesa em parte porque tem planos e capacidade para desligar as redes do país inteiro do resto do [ciberespaço](#). A China pode limitar a utilização do ciberespaço numa crise desligando os utilizadores não essenciais”.²⁷ Já os EUA não têm a mesma possibilidade. Por sua vez, a Coreia do Norte tem uma pontuação elevada, quer para ciberdefesa, quer para a ciberdependência. Isto ocorre porque o país pode desligar a sua limitada conexão ao ciberespaço ainda de forma mais fácil do que a China, não tendo praticamente redes ou sistemas informáticos dependentes de ligações ao mundo exterior.

Um dos desenvolvimentos a que se assiste nos últimos anos é a criação cibercomandos, ou comandos cibernéticos, no âmbito das forças armadas de vários países – um claro sinal que a possibilidade de uma ciberguerra está, cada vez, mais, a ser encara como uma séria ameaça. Os EUA foram pioneiros na criação de um Cibercomando (o [USCYBERCOM](#), na sigla em língua inglesa) o qual se encontra subordinado ao Comando Estratégico das suas forças armadas. Este desenvolvido parece estar a ser rapidamente imitado por outros países. Por exemplo, na Europa, as forças armadas alemãs ([Bundeswehr](#)) desenvolvem, desde 2009, a sua própria ciberforça, onde se inclui o recrutamento e treino de [hackers](#) para as coadjuvarem nesta tarefa²⁸. Em finais de 2009, a Coreia do Sul anunciou também a criação de um cibercomando, provavelmente em resposta à criação, pela Coreia do Norte, de uma unidade de guerra cibernética. Em 2010, a China lançou similar unidade, no âmbito das suas forças armadas, oficialmente dedicada à ciberguerra defensiva e segurança da informação do país²⁹.

Papel dos actores não-estatais

Um dos aspetos mais curiosos dos ciberconflitos é o protagonismo que os atores não estatais tendem a ter nestes. Tornou-se evidente, pelos incidentes já ocorridos, que certos países têm interesse em manter ou tolerar “organizações por procuração”. Estas podem, quando oportuno, ser envolvidas em atividades de ciberataques e, eventualmente, também, em atividades de ciberdefesa, se necessário. Um ataque distribuído de negação de serviço ([DDOS](#), na sigla inglesa) poderá, por exemplo, ser posto em prática por um utilizador médio de computadores, desde que disponha das ferramentas certas.

Para os estados interessados, uma vantagem desta atuação, é, desde logo, que os ataques de negação de serviço são normalmente difíceis de atribuição de autoria. Mas, tendo conta os meios técnicos necessários, que tipo de ciberataques é plausível que possam ocorrer por iniciativa exclusiva de atores não estatais e à margem dos estados? E, por similares razões técnicas, logísticas, de meios, etc., que tipo de ciberataques é plausível que só possam ocorrer com o apoio ou a anuência tácita dos estados, ainda que oficialmente estes neguem qualquer envolvimento? De acordo com Alexander Klimburg, ataques menos sofisticados que a colocação de bombas lógicas (em inglês [logic bomb](#)) mas mais visíveis do que estas, “como os ataques de negação de serviço ou os ataques que apagam páginas de um site na Web” são, frequentemente, “empreendidos por grupos não estatais atuando, pelo menos, com o seu suporte tácito” ³⁰.

Estas articulação entre atores estatais e não estatais para efeitos de ciberataques, parece existir em vários países. Um caso é o da China que integra, desde inícios da década passada, na sua organização militar, unidades preparadas para atividades de ciberguerra. Por exemplo, “a milícia da cidade de Guangzhou criou um batalhão de guerra de informação organizado em torno das instalações da empresa de comunicações dessa província chinesa. Esse batalhão abrange companhias de guerra

de redes de computadores e de guerra eletrônica". Alexander Klimburg faz notar que é possível indivíduos "fazerem parte dessa milícia sem nunca terem usado um uniforme militar. A referida estratégia chinesa coloca aos analistas ocidentais, entre outros problemas complexos, o problema das múltiplas identidades dos seus intervenientes. Assim, "é possível, para um mesma unidade de milícia de ações de ciberguerra, ser, ao mesmo tempo, um departamento de tecnologias de informação numa universidade, uma agência de publicidade [online](#), um clã de jogo [online](#), uma equipa de [hackers](#) patrióticos e um sindicato do cibercrime local envolvido em pirataria informática"³¹.

Outro caso interessante de atuação de atores não-estatais, direta ou indiretamente patrocinados pelo seu país de origem, é o caso da Rússia. A Rede de Negócios Russa é considerada a principal organização mundial no fornecimento de base logística para ciberataques e de outras atividades, sem motivações políticas, que encaixam no perfil de cibercrime. É também identificada pela [NATO](#) como uma ameaça à cibersegurança dos seus membros. Entre outras acusações que lhe têm sido feitas, consta também a da facilitação dos ciberataques à Geórgia, durante a [Guerra na Ossétia do Sul em 2008](#).

Uma guerra cibernética consiste de muitas e diferentes ameaças virtuais.³² Com a proliferação das redes de computador pelo mundo, os ataques a elas tornam-se mais complexos e perigosos.

Espionagem e violação da segurança nacional

A espionagem cibernética é um ato praticado para se obter informações sigilosas de governos de países. A violação desse sigilo pode causar muitos danos reais ao país atacado. Em uma situação de guerra física, isso se torna ainda mais perigoso, com a possibilidade de obtenção de informações sobre as táticas do inimigo. Ocorreram ataques desse tipo, os mais importantes até então foram contra os Estados Unidos. Eles receberam os codinomes de [Moonlight Maze](#), em 1998, e [Titan Rain](#), em 2003.³³ O [Comando Cibernético dos Estados Unidos](#) tenta determinar se as atividades de espionagem tem finalidade comercial, roubo de propriedade intelectual e venda de informações, ou se elas representam atividades militares contra a segurança nacional.³⁴ Os civis de um país também podem sofrer com a espionagem, tendo informações importantes descobertas, tais como número do cartão de crédito, contas em bancos, telefone, endereço, número de documentos, entre outras.³⁴

Sabotagem

As atividades militares que fazem o uso de computadores para controlar e monitorar equipamentos correm risco de sofrerem [sabotagem](#) para inutilizar possíveis ações com o uso desses equipamentos. Sistemas de comunicação também podem ser interrompidos, tais como televisão, telefone e Internet. A infraestrutura do país também pode ser alvo dos ataques, afetando o sistema de energia, trens e mercado de

ações.³⁴ Esse tipo de sabotagem também pode ocorrer à indústria, como exemplo mais relevante, tem-se o vírus [Stuxnet](#). Segundo o jornal *The New York Times*, ele é considerado "o primeiro ataque crítico a infra-estrutura industrial".³⁵

Stuxnet

O [Stuxnet](#) foi um [worm](#) projetado para atacar o sistema industrial [SCADA](#), desenvolvido pela [Siemens](#), mais especificamente o sistema de controle das centrífugas de [enriquecimento de urânio](#) do [Irã](#), em [2010](#), fazendo-as girar mais rapidamente do que o normal e causando rachaduras em seu interior sem que os funcionários percebessem o ocorrido. Como a usina não tem acesso à [Internet](#), o vírus só pode ter se infiltrado por algum dispositivo com saída [USB](#), como [pendrives](#). O maior número de computadores infectado ocorreu no [Irã](#), com o objetivo de infectar um dispositivo que fosse levado para dentro da fábrica. Esse [vírus](#) é considerado um dos mais complexos já feitos, por isso não pode ter sido produzido por um usuário doméstico, também eram necessárias informações privilegiadas sobre o funcionamento do sistema da usina, acha-se que tenha sido produzido a mando de algum governo interessado no adiamento da produção da [bomba atômica](#) iraniana. Para computadores com sistemas operacionais comuns como o [Windows](#) ou [Mac OS X](#), o Stuxnet não causa danos, sendo fácil removê-lo. Creditam-se a ele o estopim de ciberguerra, porém, antes dele, outros ataques a outros países já haviam acontecido.

Ataques ao Brasil

Espionagem do Brasil pelos Estados Unidos e Canada

De acordo com as revelações de [Edward Snowden](#), em janeiro de 2013 apenas, a [NSA](#) tinha recolhido 2,3 bilhões de dados de usuários brasileiros, tendo atividades de espionagem em setores fundamentais da economia do Brasil.^{36 37 38 15}

Em fevereiro de 2014, em discurso na cerimônia pelo centenário da [Escola de Guerra Naval](#), no Rio, o ministro da Defesa do Brasil, [Celso Amorim](#), associou o caso da espionagem do governo brasileiro pelos Estados Unidos à competição por recursos naturais.^{39 40 41}

Ataques à Estônia

A [Estônia](#) é um país "digitalizado", tem a maioria de seus serviços estatais actuando no mundo virtual e foi o primeiro país a realizar eleições pela [Internet](#). Em abril de [2007](#), quase todos esses [sites](#) governamentais foram atacados e ficaram temporariamente fora do ar, sites de jornais e emissoras de televisão também foram alvo dos ataques. Credita-se os ataques a [hackers russos](#), porém, ainda não se sabe a origem real dos ataques. A motivação para esses ataques pode ter sido a polêmica sobre a remoção da estátua de bronze de um soldado russo, para eles, a estátua

simbolizava a vitória contra o [nazismo](#), mas que para a [Estônia](#), lembrava apenas a ocupação [soviética](#) em seu território.

Ataques de chineses aos Estados Unidos

Empresas [estadunidenses](#) foram alvo de ataques [chineses](#) em janeiro de [2010](#), a principal delas o [Google](#). Esses ataques estariam relacionados com [espionagem](#) de [e-mails](#) de ativistas que eram contrários ao governo chinês. O [Google](#) anunciou que pararia as ações na [China](#), atualmente os servidores de [Hong Kong](#) recebem os acessos chineses.

WikiLeaks

A [WikiLeaks](#) é um site que, alimentado por colaboradores e informantes, divulga pela [Internet](#) documentos secretos obtidos por diferentes meios e que sejam considerados por seus administradores de interesse público. Seu fundador, [Julian Assange](#), está atualmente preso na [Inglaterra](#) acusado de abusos sexuais ocorridos na Suécia; porém, seus seguidores e outras pessoas ligadas à defesa da liberdade de expressão e das liberdades individuais afirmam que o motivo real para sua detenção foi o site [WikiLeaks](#). Fundado em dezembro de [2006](#), mas somente divulgado amplamente em [2010](#), recebia doações pela [Internet](#), como [Visa](#) e [PayPal](#), e estava hospedado em servidores da [Amazon](#). Tais sistemas de doações e a [Amazon](#), após a grande repercussão obtida pelo site e as muitas polêmicas - em especial envolvendo o governo dos Estados Unidos, principal alvo das denúncias do site -, decidiram desfazer as parcerias com o [WikiLeaks](#), o que causou a fúria dos seus colaboradores. Essas empresas passaram a ser alvos de ataques de pessoas ligadas a [Julian Assange](#). Todavia, não se tratou, a rigor, de uma ciberguerra, mas de um ativismo em rede sob forma de protesto.^[1] Atualmente, a [WikiLeaks](#) é hospedada em vários domínios e todos os documentos são de acesso livre, dando ao usuário o direito de salvá-los no próprio computador

2013 Revelações dos Programas Americanos de [Vigilância global](#)

Em junho de 2013, se tornou conhecimento mundial o fato de que os Estados Unidos vem operando sistemas de monitoramento e vigilância maciça das comunicações eletrônicas em todo o mundo. Os programas de vigilância global têm vários objetivos e capacidades, entre elas a de interceptar comunicações por e-mail, voz, vídeo, fax-símile e qualquer outro meio de comunicação em qualquer parte do mundo.^[1]

A montagem do sistema de vigilância global coincide com a construção da hegemonia norte-americana a partir da segunda metade do século XX. Com a perda do poderio econômico estadunidense, a [CIA](#) e a [NSA](#), passaram também a espionar empresas estrangeiras^[2] e a repassar informações privilegiadas obtidas pelo Echelon às

corporações americanas e aos aliados no monitoramento global, os membros do grupo chamado [The Five Eyes](#), a saber: [Reino Unido](#), [Irlanda](#), [Austrália](#), [Canadá](#) e [Alemanha](#), que é um sistema geopolítico de espionagem eletrônica dos EUA, controlado pela [NSA, Agência de Segurança Nacional](#) americana.^[3]

[Operações de acesso adaptado \(TAO\) NSA](#) é a divisão de coleta de inteligência para [Ciberguerra](#) da agência americana [NSA](#), em funcionamento desde 1998 ao menos. [Operações de acesso adaptado \(TAO\) NSA](#) identifica, monitora, infiltra, e reúne informações sobre sistemas de computadores sendo usado por entidades fora dos Estados Unidos. ^[4]^[50]

A NSA se refere a tais atividades como "de exploração de rede de computadores", ou (CNE), [acrônimo](#) para "computer network exploitation", em inglês. Um documento revelado por [Edward Snowden](#) descrevendo o trabalho da unidade, diz que TAO tem modelos de software que lhe permite invadir os [hardware](#) comumente utilizados ao redor do mundo, incluindo [Roteadores](#), [comutadores de rede](#), e [Firewalls](#) de vários fabricantes.

De acordo com o [The Washington Post](#), os engenheiros da TAO, são considerados "a elite de [Hackers](#) da [NSA](#), ^[51] e preferem atacar [redes de computadores](#) ao invés de computadores isolados, porque tipicamente há muitos dispositivos em uma única [rede](#).

Revelações de [Edward Snowden](#) publicadas no [Der Spiegel](#) em 29 de Dezembro de 2013, mostram que a unidade possui um catálogo interno ^[52], onde são listados os artefatos disponíveis as agências de inteligência para invasão de sistemas computacionais. O catálogo enumera os inúmeros dispositivos eletrônicos para atingir os usuários finais que vão desde [Backdoors](#) a implantes no próprio [Hardware](#), em cabos, [Conectores](#) e outros. ^[52] Os dispositivos criados pela divisão, se destinam a criar e desenvolver meios de [Hacking](#). Esta se tornou a divisão da NSA de maior expansão recentemente, dedicada especialmente a criar tais dispositivos.^[51]^[52]

As operações da [TAO](#) são consideradas pela agência como extremamente bem sucedidas, incluindo acesso via [Backdoor](#) a varios sistemas de [Smartphones](#), incluindo ao [iPhone](#), mostram documentos publicados no [The Washington Post](#). ^[53] Em 29 de março de 2014, o jornal [Der Spiegel](#) publicou documentos que mostram que como parte do programa de [Vigilância Global](#) que inclui a [Vigilância de Computadores e Redes](#), os sistemas de satélite da [Alemanha](#) se tornaram alvo de espionagem feita pelo [CGHQ](#), membro do conhecido grupo chamado [Five Eyes](#), Cinco Olhos, em português.^[52]

Empresa detecta supervírus espião e 'indício de guerra cibernética'

A Symantec, uma das principais empresas de segurança da informação do mundo, anunciou no domingo ter descoberto um vírus de computador que pode ter sido desenvolvido para ataques cibernéticos contra servidores de governos.

Batizado de Regin, o vírus é, segundo a Symantec, o mais sofisticado programa invasor já visto. A empresa disse ainda que o Regin foi usado para ataques nos últimos anos contra uma variedade de alvos ao redor do mundo, entre organizações governamentais, empresas e usuários comuns.

Computadores na Rússia, Arábia Saudita, México, Irlanda e Índia foram os mais afetados, ao lado de Irã e Paquistão.

Usuários privados e pequenas empresas corresponderam a 48% dos ataques detectados, à frente de empresas de telecomunicações (28%).

Pesquisadores da Symantec disseram que o vírus pode ter levado anos para ser desenvolvido. Isso sugere que tenha sido "encomendado" por algum governo.

"O vírus parece ter vindo de alguma organização do Ocidente, em função do nível de habilidade requerido para o seu desenvolvimento em termos de investimento de tempo e recursos", afirmou à BBC Sian Jenkins, especialista da Symantec.

Ele disse acreditar que o Regin foi usado "de forma sistemática para coletar informações e em operações de vigilância".

A Symantec viu no Regin paralelos com o Stuxnet, vírus descoberto em junho de 2010 e supostamente criado a mando de autoridades americanas e israelenses para sabotar o programa nuclear do Irã.

Mas enquanto o Stuxnet atuava danificando equipamentos, o Regin parece ter sido criado para coletar informações: segundo a Symantec, o vírus pode capturar imagens de telas, roubar senhas ou mesmo recuperar arquivos apagados.

Segundo a Symantec, a principal faceta da sofisticação do Regin é a dificuldade de detecção mesmo com alguns dos mais sofisticados programas antivírus do mercado. Outro problema é que ainda não se conhece toda a capacidade do vírus.

Cientistas criam vírus de computador que se espalha pelo ar 'como gripe'

Dave Lee Repórter de Tecnologia da BBC - 26 fevereiro 2014



Redes

Cientistas de Liverpool, no Reino Unido, criaram um tipo de vírus de computador capaz de se espalhar pelo ar, por redes wi-fi, como "uma gripe comum".

Em áreas densamente habitadas, onde há muitas destas redes sem fio, o vírus pode ir de rede em rede, procurando por suas falhas.

Uma vez no controle de um ponto wi-fi, o vírus deixa vulneráveis os computadores conectados a esta rede .

O chefe da equipe de pesquisadores disse à BBC que o objetivo é criar um programa de computador capaz de evitar que esse tipo de ataque seja possível.

"Em vez de esperar que as pessoas criem senhas fortes, é melhor integrar sistemas capazes de detectar intrusos nesses pontos de acesso", disse Alan Marshall, professor de redes de comunicação da Universidade de Liverpool.

Ele não quis entrar em detalhes sobre os métodos usados para prevenir o uso desse tipo de ataque, mas disse que a tecnologia necessária para testar esses métodos foi criada na universidade.

Sob controle

Chamado de "camaleão", o vírus procura por pontos de acesso a redes sem fio - aparelhos que transmitem o sinal wi-fi - que não tiveram suas senhas de fábrica alteradas.

Essa senha é diferente das usadas para se conectar à rede sem-fio propriamente dita e, com frequência, não são alteradas por quem compra esses aparelhos.

Isso dá controle do ponto de acesso ao hacker, que pode acessar os computadores conectados à rede para roubar informações.

Disseminação

Mas é o próximo passo do vírus que é mais incomum.

Uma vez instalado no ponto de acesso, o vírus pode - sem ser controlado por um humano - buscar automaticamente outros pontos de acesso vulneráveis para assumir seu controle.

Marshall disse à BBC que é improvável que isso represente uma ameaça às redes wi-fi de grandes empresas, já que elas normalmente têm muitos mecanismos de segurança.

No entanto, redes domésticas ou de empresas menores, como restaurantes e bares, não costumam ter esses mecanismos.

Segundo o cientista, como sua equipe conseguiu provar que a ameaça é real, o foco agora é criar um programa capaz de prevenir esse sequestro de redes sem fio.

Inimigos invisíveis: a guerra cibernética

Mesmo diante de oponentes como China, Rússia e também terroristas, EUA elegem guerra cibernética como principal ameaça



Oficiais atualizam proteção anti-hackers da central de controle da base aérea de Barksdale, nos EUA (Foto: Tech. Sgt. Cecilio M. Ricardo Jr/US Air Force)

Nos Estados Unidos, a guerra cibernética é considerada, hoje, a principal ameaça à segurança nacional, maior até mesmo que a rival Rússia, a ameaçadora China ou os extremistas islâmicos, revelou no Senado o professor Gunther Rudzit, coordenador do curso de Relações Internacionais da Fundação Armando Álvares Penteado (Faap), citando a declaração ouvida de um pesquisador norte-americano na área de defesa. A guerra cibernética é levada tão a sério, disse, que o Departamento de Defesa criou sua própria divisão de combate cibernético.

Segundo ele, a divisão voltada para a guerra cibernética emprega jovens ligados a essa nova realidade para buscarem falhas e formas de minar os sistemas de defesa das potências adversárias. Os americanos reconhecem, explica o professor, que as ações militares estão cada vez mais dependentes do aparato tecnológico, e os sistemas que alimentam passaram a ser um calcanhar de aquiles até mesmo para a maior potência bélica do planeta.

“Quebrada essa estrutura de comando e controle baseada em tecnologia, para de funcionar a guerra moderna. Você está num tanque, numa tela, clicando o que outra unidade está vendo, o que um avião está vendo. Se você quebra isso, eles param e deixam de funcionar, como essa máquina de guerra que eles têm. Então, tecnologia passa a ser, hoje em dia, algo fundamental”, raciocina Rudzit sobre a guerra cibernética.

O senador Fernando Collor, que alertou sobre esse tema da guerra cibernética durante os debates realizados na CRE, lembrou que o Ministério da Defesa norte-americano (o Pentágono) já considera como ato de guerra contra o país qualquer ataque cibernético aos seus sistemas de defesa, ou mesmo aos sites de governo na internet, devido ao potencial de dano que essas ações podem causar.

“Por mais armamentos que se tenha, por mais poderosa que seja uma armada, uma força terrestre, uma força aérea, nós temos hoje esse outro elemento que é fortíssimo, que é o chamado ciberterrorismo ou ataque cibernético. Quem está preparado para se defender de algum ataque cibernético?”, desafiou, nesse aspecto da guerra cibernética, o senador.

Sem preparação

O professor Rudzit lembra que a maioria dos países já está empenhada em se preparar para a guerra cibernética. “Organizações terroristas adorariam quebrar toda a rede de eletricidade da costa leste americana. Imagine o caos!? E se for a rede bancária?”, especulou, citando um tipo de ataque da guerra cibernética. Como admitiu o especialista, tais ataques de proporções incalculáveis podem ser desfechados por uma única pessoa, “um rapazinho de 15 ou 16 anos”, a partir de sua casa.

O general Aderico Mattioli, director do Departamento de Produtos de Defesa do Ministério da Defesa, vê o país em risco também nesse aspecto da guerra cibernética. Os sistemas bancários e as redes por onde passam conhecimentos estratégicos e essenciais estariam expostas pela falta de um simples programa antivírus genuinamente nacional, imune a contra ordens do fabricante que possam expor a segurança nacional.

“Deveríamos ter, no mínimo, a capacitação em bancos escolares, na educação, para formarmos também uma capacidade produtiva e o entendimento de produto de defesa, que não é mais aquele produto materializado propriamente dito. A cibernética, talvez, seja a mais vulnerável na nossa realidade e a mais exequível a curto prazo, a que demande menos recurso para darmos um grau de proteção — vamos chamar de firewall — mínimo necessário para o país. É uma área com a qual podemos contribuir muito”, explicou o general sobre a guerra cibernética.

Em meados de Fevereiro passado, o Exército anunciou a aquisição de novos programas de computador para segurança e prevenção contra a guerra cibernética, como parte de planejamento para criar sistema de defesa e contra-ataque a possíveis ameaças a páginas e redes institucionais e de protecção a dados sensíveis. Em

janeiro, as Forças Armadas realizaram duas licitações para a compra de antivírus e de programa que simula ataques cibernéticos, a serem desenvolvidos por empresas brasileiras. Serão investidos R\$ 6 milhões.

“Os ataques que registramos até agora são parecidos com os que acontecem em qualquer empresa. Tentativas de roubos de senhas, negações de serviço etc. Mas o modo como se obtém uma senha de banco é o mesmo que se pode usar para obter dados confidenciais do Exército. E já tivemos sites do governo derrubados”, disse à imprensa o general Antonino Santos Guerra, diretor do Centro de Comunicações e Guerra Eletrônica do Exército (Ccomgex), admitindo que o país tem hoje preparo mínimo para cenários da guerra cibernética. “Temos uma grande rede, a EBnet, que reúne os quartéis em todo o país e ela está bem blindada, mas há pontos de vulnerabilidade”, explicou.



General Santos Guerra, do Ccomgex: país tem hoje preparo mínimo para cenários de ataque cibernético (Foto: Roberto Jayme/Valor)

A Ccomgex faz parte do Centro de Defesa Cibernética do Exército (CDCiber), criado em 2010 para concentrar a administração de todas as ações de proteção virtual da organização. O orçamento previsto para o CDCiber em 2012 é de R\$ 83 milhões, que devem ser destinados a pelo menos outras quatro aquisições que incluem equipamentos, softwares e o treinamento de pelo menos 500 oficiais.

Sem preparação

Professor da Divisão de Assuntos Científicos e Tecnológicos da Escola Superior de Guerra (ESG), Simon Rosental afirmou que as potências mundiais não querem permitir que o Brasil e outros países emergentes tenham acesso ao que se chama de “tecnologias sensíveis”. O alerta teria sido dado ainda em 1996, durante congresso

internacional sobre tecnologias sensíveis realizado no Rio de Janeiro e patrocinado pela ONU e pela Subsecretaria de Inteligência da Presidência da República.

“Os países desenvolvidos colocaram claramente: ‘Brasil e demais países que possuem riquezas naturais em abundância não vão avançar em tecnologias sensíveis’. Vocês ficam com bens de baixo conteúdo tecnológico e valor agregado. Tecnologias sensíveis ficam conosco, porque, como podem ser aplicadas para o bem e para o mal, vocês poderão fazer mau uso”, relatou o professor.

“Essa conferência não foi tranquila. Tanto o Brasil como os demais países em desenvolvimento não se conformaram com uma situação dessas. Se já temos um hiato tecnológico grande em relação aos países desenvolvidos, e a tecnologia está avançando cada vez mais, a velocidades maiores, se aceitarmos uma barbaridade dessas, cada vez vamos andando para trás e cada vez vamos ficando mais distantes da tecnologia”, afirmou Rosental.

Prejuízos e temor

Em comunicado à imprensa, o Gabinete de Segurança Institucional da Presidência (GSI) disse, sobre a guerra cibernética, que “os ataques mais preocupantes são aqueles que visam acesso indevido a informações sigilosas da administração pública federal” e afirmou que a preparação do órgão contra possíveis ataques tem sido adequada.

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (Cert), que reúne sobre a guerra cibernética, notificações de ataques eletrônicos em todo o país, o Brasil registrou quase 400 mil ataques a computadores em 2011 (veja infográfico abaixo). O total de notificações recebidas em 2011 foi quase 300% maior que em 2010.

Cerca de metade das fraudes registradas, segundo o Cert, foram páginas falsas, geralmente de bancos, criadas para roubar dinheiro dos usuários. Segundo a Federação Brasileira dos Bancos (Febraban), as fraudes cibernéticas custaram R\$ 685 milhões aos bancos só no primeiro semestre de 2011, 36% a mais do que no mesmo período em 2010.

400 mil ataques somente no ano passado

Notificações de incidentes na internet, como tentativas de fraudes ou agressões a redes e páginas, quase triplicaram em 2010

	Incidentes	em 2011	%*	Legenda
	Worm	26.897	6	Processo automatizado de propagação de códigos maliciosos na rede
	DoS	272	0	Denial of Service: ataques tiram do ar um serviço, computador ou rede
	Invasão	106	0	Acesso não autorizado a um computador ou rede
	Web	15.491	3	Comprometimento de servidores web ou desfigurações de páginas na internet
	Scan	119.755	30	Varreduras em redes de computadores, amplamente usadas para identificar potenciais alvos vulneráveis
	Fraude	40.381	10	Incidentes em que ocorre tentativa de se obter vantagem
	Outros	196.613	49	
	Total	399.515	100	

* Valores aproximados

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (Cert), mantido pelo Comitê Gestor da Internet no Brasil

O que todos devem saber sobre guerra cibernética

Por: [Andy Manoske - Quora](#)

31 de Dezembro de 2014



A guerra cibernética consiste, basicamente, no uso de ataques digitais às estruturas *estratégicas* ou *táticas* de um alvo, para fins de *espionagem* ou *sabotagem*. Vamos entender isso mais a fundo.

O básico

Planejamento estratégico e tático

“Estratégico” e “tático” são termos bastante usados entre militares que significam, basicamente, “coisas que ajudam os países a expressar suas vontades políticas e/ou declarar guerra”. Aí estão inclusas várias coisas: armas, munição e combustível para jatos e aviões. Há também coisas menos óbvias no meio: a moral das tropas, a visão política do público civil, e o bem-estar econômico do país.

Deve-se destacar a diferença entre o nível *estratégico* e o nível *tático*. Em termos militares, o nível tático se refere ao que está sendo utilizado diretamente no combate.

O nível estratégico está acima do tático; em outras palavras, ele consiste no que é necessário para vencer uma guerra, e não apenas batalhas e confrontos específicos. Isso inclui os recursos necessários para manter uma guerra: suprimentos, armas,

munição, fábricas, homens e mulheres saudáveis para a linha de frente das batalhas, e uma população interessada em manter a guerra.



Se a guerra fosse um jogo de xadrez, o nível tático se resumiria ao movimento de cada peça para capturar os inimigos. O nível estratégico refere-se ao modo como você ganha o jogo e destrói o seu oponente.

Lembre-se da diferença entre o nível tático e estratégico. Essa diferença será muito importante no final desse artigo, quando responderemos uma importante pergunta: por que a guerra cibernética é uma ameaça para a sociedade?

Espionagem

A espionagem consiste basicamente em capturar informações destinadas a outras pessoas. No caso de uma ciberguerra, os espiões roubam informações táticas e estratégicas — dados sobre a movimentação de tropas, os pontos fortes e fracos do sistema bélico do país e qualquer outra informação valiosa sobre recursos necessários para a guerra.

Sabotagem

Também conhecida como “ação direta”; isto é, quando alguém resolve ser proativo e fazer algo com as próprias mãos. Na ciberguerra, a sabotagem pode ir de uma ação

simples – derrubar os servidores de um site governamental – a algo extremamente nocivo, como causar o derramamento nuclear de uma ogiva.

É um termo muito amplo, mas tudo o que você precisa lembrar é que ele se resume a “fazer algo” – ao contrário da espionagem, que se resume a “descobrir algo”.

Como funciona

Hackers com apoio do Estado – sejam membros das forças militares de um país, ou financiados por tal país – atacam computadores e redes do oponente que afetem recursos necessários para a guerra.

Eles fazem isso da mesma forma que em qualquer outro computador ou sistema: eles estudam o sistema profundamente, descobrem suas falhas e usam essa falhas para controlar esse sistema ou destruí-lo.



O caça J20 PLAAF de quinta geração, ao lado do caça USAF F-22. Existem teorias que afirmam que o design do J20 foi inspirado em documentos confidenciais obtidos a partir da ciberespionagem.

No primeiro caso, podemos usar informações confidenciais destinadas a outrem (espionagem) para ganhar a dianteira na batalha contra seu adversário. Podemos descobrir a velocidade de um míssil e construir um avião que possa ultrapassá-lo. Podemos descobrir para onde um alvo está movendo suas tropas, e planejar uma emboscada. Podemos descobrir quais cientistas são importantes na criação dessas

armas, ou qual político foi impensável na arrecadação de fundos para o tal sistema bélico — e atacá-los diretamente.

Quando se tem o controle desses sistemas, sabotar pessoas também é possível. E se eu colocasse um programa secreto no código-fonte de um míssil que me permita explodi-lo enquanto ele está na terra? E se eu pudesse descobrir como as tropas estão se comunicando, e assim ganhar acesso à rede para que eu possa confundi-los e invadir a base deles?

Ou pior: e se eu atacasse funcionários civis e políticos de um país envolvido em uma ação militar? Eu poderia invadir seus sistemas/contas e fraudá-los, me passando por um deles. Eu também poderia usar essas informações para controlá-los e forçá-los a trabalhar para mim: por exemplo, chantageá-los por causa de algo que achei no computador, ou sequestrar suas famílias usando informações privadas.

Destruir esses sistemas tem um resultado óbvio: você destrói o que controla esse sistema, e, conseqüentemente, impede-o de funcionar. Um exemplo comum de ciber guerrilha é o uso de ataques DDoS (ataque distribuído de negação de serviço) para desativar sites governamentais e redes sociais. Essa tática foi usada efetivamente pelos russos durante a Guerra da Ossétia do Sul em 2008, causando caos e espalhando informações falsas para a população antes e durante a invasão russa.

Quem são os alvos

A guerra cibernética tem como alvo qualquer setor importante para a infraestrutura do inimigo. Isso significa setores óbvios como o exército, a defesa nacional e a indústria bélica. No entanto, esses alvos também podem ser fábricas civis de armas, minas e outras manufaturas que auxiliem no funcionamento dessas fábricas — e o sistema elétrico, que fornece energia para todos esses setores.

Na sua versão mais assustadora, a ciber guerra pode ter como alvo o recurso estratégico mais importante de um país: sua população. Um hacker poderia fazer um ataque terrorista para desestabilizar ou desmotivar uma população a lutar. Isso implica em coisas assustadoras como ataques aos setores financeiros, que causariam danos econômicos; ou ataques a sistemas de comunicação — imagine o que aconteceria se a rede de telefonia fosse desativada e a internet caísse.

Por que isso ameaça a sociedade

Na minha opinião, a guerra cibernética é assustadora por dois motivos. Primeiramente, a ciber guerra estratégica não faz nenhuma distinção entre alvos civis e militares.

Assim como as armas nucleares da Guerra Fria, as armas digitais podem atingir, indiscriminadamente, alvos civis e militares. Apesar de um míssil causar um dano muito maior do que um vírus, um ciberataque pode, sim, resultar em perdas e mortes de civis.

Um bom exemplo seria um ataque ao sistema energético. Nos EUA, este é um recurso estratégico importantíssimo. Se o sistema fosse destruído por um ciberataque (uma possibilidade que assusta o país), não seriam só as fábricas de armas que parariam de funcionar. Um ataque desses resultaria também em acidentes de trânsito, cirurgias interrompidas, falhas em máquinas de suporte à vida — basicamente, uma quantidade absurda de pessoas morreriam.

Em segundo lugar, é muito difícil descobrir o autor de um ciberataque; dessa forma, os governos que financiam esses ataques não tem que lidar com as consequências de suas ações.

Um aspecto que faz as armas digitais piores do que as armas nucleares é a atribuição — descobrir quem fez o ataque. É muito fácil esconder a origem de um ataque desses, graças a *proxies* que mascaram a identificação do autor dos ataques. Mesmo que o governo descubra de qual computador o ataque foi efetivado, ainda existe a dificuldade de descobrir quem era a pessoa atrás da tela — e é ainda mais difícil saber se ele era, ou não, um agente do governo.

Sem atribuição, não há responsabilidade. E sem responsabilidade, não existem coisas como intimidação e cessar-fogo. Se um governo não pode ser culpado por ciberataques, existe sempre a possibilidade de este país ir além e partir para ataques semi-terroristas, como a interrupção do serviço elétrico de um país, ou ataques físicos (e perigosos) a fábricas e cidades.

Em ambos os casos, cidadãos inocentes podem correr riscos.

Quantos desses ataques são financiados por governos

Para ser honesto, ninguém sabe.

Não existem estatísticas sobre a divisão entre ciberataques financiados por países e ataques financiados por estados dissidentes ou movimentos como a Al-Qaeda. Esse é um dos maiores problemas da ciberguerra: ela é assimétrica por natureza. Um país pequeno com um forte grupo de hackers pode facilmente atingir um país enorme com uma infraestrutura fraca e um exército incrível.

É razoável assumir que hackers financiados por países ricos são mais perigosos. A maioria dos países de primeiro mundo sabe se defender de ciberataques básicos. Hackers financiados por países poderosos são, em sua maioria, mais bem-

preparados, e podem organizar ataques que ultrapassam essas defesas, causando danos catastróficos.

Artigos organizados em 17 de Abril de 214

Por: Hilário Langa