O Carácter Trinitário da Guerra no Ciberespaço

Tenente-coronel
Rui Manuel Piteira Natário

Introdução

A validade das ideias de Clausewitz tem sido questionada pelo progresso tecnológico, mais concretamente pelo surgimento das armas nucleares ou pelo alargamento da conflitualidade a novas dimensões inimagináveis no seu tempo. O surgimento das redes telemáticas, como sustentáculo das novas formas de comunicação, reduziu as distâncias e abriu todo um novo leque de possibilidades para o relacionamento belicoso entre as forças políticas, ideológicas e financeiras que moldam a realidade contemporânea. As notícias sobre ataques cibernéticos surgem com cada vez maior frequência nos cabeçalhos e esta sistemática exploração de diversas falhas de segurança é uma grande preocupação para muitas nações que tentam arquitectar estratégias para contrariar esta realidade.

Isto mostra que a moderna conflitualidade decorre num novo ambiente operacional, com regras completamente novas, em que o ciberespaço é um campo de batalha onde decorrem operações que vão da disseminação de propaganda até à mais sofisticada espionagem, passando por ataques directos contra diversas infra-estruturas. No entanto, embora o impacto da tecnologia tenha sido decisivo na mudança do pensamento estratégico, a natureza da guerra não se alterou nos seus princípios fundamentais tal como foram enunciados por Clausewitz.

Clausewitz Revisitado

Carl von Clausewitz é, sem dúvida, um dos mais destacados pensadores na área da arte militar e do estudo teórico da guerra. Na sua obra-prima *Da Guerra* [7], explanou as suas análises dos conflitos bélicos do seu tempo e as conclusões a que chegou mantêm ainda hoje uma surpreendente actualidade. A referida obra é um dos mais citados e respeitados clássicos no âmbito da estratégia e continua a exercer grande influência em todos os

estudos modernos sobre o tema, sendo incontornável no ensino destas matérias em diversas academias militares. A sua concepção assenta no princípio de que as guerras nascem exclusivamente das relações políticas entre governos e nações, chegando mesmo a afirmar, numa das suas mais conhecidas citações, que a guerra nada mais é senão a continuação das relações políticas, com o complemento de outros meios [7]. Ao longo da obra, Clausewitz recorre a diversas analogias para ilustrar o seu pensamento comparando, por exemplo, a guerra a um camaleão que modifica a sua natureza em cada caso concreto [7].

No entanto, aquilo que nos interessa analisar neste trabalho é o carácter trinitário que Clausewitz postulou para a guerra. Segundo ele, a guerra é uma surpreendente trindade em que se encontra, primeiro que tudo, a violência original do seu elemento, o ódio e a animosidade, que é preciso considerar como um cego impulso natural, depois, o jogo das probabilidades e do acaso, que fazem dela uma livre actividade da alma, e, finalmente, a sua natureza subordinada de instrumento da política por via da qual ela pertence à razão pura [7].

Assim, Clausewitz caracteriza a guerra como um fenómeno total cujas tendências dominantes podem ser genericamente caracterizadas como a violência irracional e ódio, o acaso e a oportunidade e por último, a razão. Continuando a sua análise, liga estas três tendências a três grupos de actores humanos; a irracionalidade ao povo, o acaso ao exército e aos seus comandantes, a quem cabe navegar nos mares da incerteza do campo de batalha, e a subordinação dos objectivos militares aos imperativos políticos faz com que a última tendência seja relacionada com o governo. E assim, as três tendências primordiais correspondem a três corpos sociais representativos: o carácter e a disposição do povo, a perícia e competência dos militares e a sabedoria e inteligência dos governantes [11].

Clausewitz acreditava que a vitória pode apenas ser alcançada através de um equilíbrio destas três componentes e conclui que o resultado final de uma guerra nem sempre pode ser considerado como definitivo [7] o que, parece ser uma outra referência ao carácter trinitário da guerra, uma vez que a vitória não é absoluta mas sim dependente da legitimidade do governo, do apoio do povo e da eficácia dos militares [26].

A Modernidade de Clausewitz

Clausewitz retratou a natureza da guerra em termos das já referidas três tendências, ou forças: a hostilidade primária, que pode levar a uma escalada descontrolada do conflito; o acaso e a incerteza, que desafiam as doutrinas e tornam a guerra imprevisível; e a racionalidade, que tenta utilizar a guerra com um propósito, para alcançar um fim. De facto, esta moldura teórica é exacta porque encontramos estas forças, em diversos graus, em todas as guerras, antigas ou modernas, convencionais ou não [10].

Assim, a natureza da guerra reside na intersecção entre o primordial sentimento da paixão, o reino das probabilidades e do acaso e a busca racional de um determinado

objectivo [16]. Estas tendências, na concepção de Clausewitz, correspondem genericamente a três instituições; a primeira à populaça, a segunda aos militares e a terceira ao governo. No entanto, cada uma destas instituições assume diferentes formas em diversas épocas e devem assim ser consideradas no seu sentido lato [10]. Ou seja, a populaça refere-se aos povos de qualquer cultura ou sociedade em qualquer momento da história. De modo semelhante, os militares representam não apenas os exércitos treinados e semiprofissionais da era napoleónica, mas qualquer outro corpo guerreiro em outra época. O governo significa qualquer corpo dirigente, ou qualquer entidade que exerça liderança de tipo político e social. Assim, o governo pode ser um estado, ou outro actor não-estado, como um clã, grupo religioso ou etnia. Em suma, a trindade consiste em forças ou tendências, que são universais, e não em instituições, que são meramente representações dessas forças [10].

Embora a segunda trindade do povo, militares e governo possa ter uma aplicação limitada, uma vez que nem todas as guerras modernas envolvem estes elementos, a primeira trindade é intemporal e de aplicação universal [16]. Paixão, probabilidade e objectivos, caracterizam todos os conflitos contemporâneos, sejam eles guerras civis, violência étnica ou a guerra ao terrorismo. As razões fundamentais que levam ao surgimento das guerras, e a razão pelas quais estas são ganhas ou perdidas, explicam-se por esta trindade [16]. Clausewitz considerava as tendências como universais – comuns a todas as guerras – e, de facto, podemos identificá-las na actual guerra ao terrorismo [10].

A Al-Quaeda desenvolve grandes esforços para mobilizar a hostilidade da sua base popular de apoio, e esta hostilidade é, de facto, uma força poderosa. Por outro lado, algumas sondagens mostram que a opinião pública tem dúvidas acerca do sucesso da guerra contra o terrorismo e muita desta incerteza tem mais a ver com as dúvidas na capacidade para atingir o estado final desejado (instalação de regimes democráticos) que com as baixas sofridas. Além disso, os objectivos da guerra ao terrorismo são simultaneamente seculares e religiosos uma vez que nem todos os actores partilham da visão jihaidista da Al-Quaeda e buscam apenas objectivos políticos [10]. Assim, temos um exemplo moderno da aplicabilidade prática da trindade de Clausewitz a um conflito não convencional, o que demonstra a contemporaneidade das suas ideias.

A Trindade e a Tecnologia

O ritmo alucinante do progresso tecnológico das últimas décadas tornou este assunto absolutamente incontornável em qualquer debate sobre os desafios contemporâneos na área da defesa. Entrando em linha de conta com a análise teórica da própria tecnologia e com os seus efeitos práticos, torna-se particularmente relevante analisar a questão de saber se a teoria da guerra de Clausewitz foi ou não tornada obsoleta pelo progresso tecnológico. Quer se trate da tecnologia que resulta em novos sistemas de armas ou na que dá origem a novas formas de actuação, este assunto está irremediavelmente no centro da discussão e da tomada de decisão relativamente aos conflitos presente e futuros.

A sociedade da informação assiste a um conjunto de desenvolvimentos tecnológicos que podem vir a tornar obsoletos os princípios tradicionais do combate. A eficácia táctica dos sistemas militares desenvolve-se à medida que a tecnologia evolui e isto é bem patente na profusa literatura existente sobre o conceito de *Revolution in Military Affairs* (RMA) [26]. Quer isto represente ou não uma revolução, é certo que enfrentamos mudanças tecnológicas que terão um impacto significante na futura doutrina militar [4]. Existem pelo menos três conjuntos de transformações impulsionados pela tecnologia que afectam a relação entre os militares e a esfera política: em primeiro lugar, alterações na natureza da relação entre os comandantes no terreno e as autoridades de comando nacional, em segundo lugar, uma expansão no contexto político da acção militar e em último lugar, mudanças na natureza da própria esfera pública [5].

Por um lado, a noção da existência de uma trindade entre o povo, o governo e os militares é pouco susceptível a estes desenvolvimentos uma vez que continua a constituir o enquadramento no qual a guerra pode ser entendida aos níveis de análise estratégica e politica [26]. Esta trindade implica que o comandante é o responsável por conduzir o seu exército através da incerteza das operações tácticas enquanto a responsabilidade de estabelecer os objectivos políticos recai sobre o governo. O impacto dos desenvolvimentos tecnológicos nos sistemas de comando e controlo podem enfraquecer esta relação, diluindo a distinção entre a acção militar e a orientação política [26]. A evolução dos sistemas de informação e comunicação resulta numa redução do atraso das comunicações e aumenta a sensibilidade de cada um dos componentes em relação aos outros [4]. O que estes desenvolvimentos sugerem é a diminuição da distância entre a liderança política, os comandantes militares e as tropas no terreno. A informação acerca dos acontecimentos no terreno flui para a retaguarda muito mais depressa, em grande volume e por uma multitude de canais. Os combatentes terão uma maior consciência dos requisitos políticos e quem está na retaguarda terá uma melhor noção dos desenvolvimentos militares em curso e do seu possível impacto [5].

Por outro lado, o impacto da tecnologia sobre os três elementos da trindade não deve ser menosprezado. No mundo contemporâneo em geral, e nos países desenvolvidos em particular, a dependência da tecnologia moderna não é vista como um luxo, mas antes como uma necessidade onde as três tendências estão intrinsecamente dependentes do ciberespaço, de uma forma ou de outra [24] e estas tendências interagem extensivamente entre elas e têm uma relação que está em permanente mutação. A tecnologia, de facto, está presente em todos os elementos da trindade sem alterar as suas relações, acelerando o ritmo de transmissão de informação e fornecendo-a em novas formas, reduzindo ou expandindo o tempo de tomada de decisão. Mas os decisores continuarão a receber uma vasta quantidade de informação através de filtros de subjectividade e assim, as suas decisões serão afectadas pelo seu juízo e este será moldado pelas forças políticas [11].

Apesar dos avanços revolucionários na tecnologia, a trindade permanece relevante para as guerras do futuro. O progresso tecnológico não irá alterar o enquadramento da guerra uma vez que afecta a gramática da mesma e não a sua lógica. Por outras palavras, as novas tecnologias podem apenas alterar a forma da guerra e não a sua natureza [11]. A

estrita subordinação dos objectivos militares aos imperativos políticos pode vir a ser influenciada pelo progresso mas, enquanto os avanços tecnológicos da sociedade de informação continuam, a natureza da guerra a nível estratégico irá permanecer inalterada. [26]. Parafraseando a analogia do camaleão, que Clausewitz usa para ilustrar o carácter de mutação da guerra, a tecnologia representa apenas uma mudança de cor [4].

O Ciberespaço Trinitário

O ciberespaço é hoje parte integrante da vida de muitos milhões de cidadãos em todo o mundo que nele mergulham para trabalhar ou apenas para se divertirem. Se para todos estes cibernautas o acesso a este mundo virtual é um dado adquirido, para muitos outros ele nem sequer existe. Apesar do seu crescimento exponencial e da sua dispersão geográfica, a distribuição física das redes de comunicações está ainda longe de ser uniforme em todas as regiões do planeta. Esta desigualdade na distribuição dos pontos de acesso tem impacto na experiência proporcionada aos cibernautas que são assim uma população diferenciada, tanto em termos técnicos como sociais. No entanto, a banalização das telecomunicações móveis confere ao ciberespaço um carácter de uniformidade que permite uma quase total abstracção do seu suporte físico.

Internet e Ciberespaço

Os últimos anos foram uma fase de crescimento verdadeiramente explosivo das tecnologias de informação, nomeadamente da Internet. Na sequência desta expansão, o termo ciberespaço passou a ser vulgarmente utilizado para descrever um mundo virtual que os utilizadores da Internet habitam quando estão *online*, acedendo aos mais diversos conteúdos, jogando ou utilizando os variadíssimos serviços interactivos que a Internet disponibiliza. Mas é fundamental distinguir o ciberespaço das redes telemáticas, pois existe uma generalizada confusão conceptual. A telemática produz a comunicação à distância, via informática, enquanto o ciberespaço é um ambiente virtual que se serve destes meios de comunicação sendo hoje uma expressão genérica para o espaço digitalizado criado e mantido pelas ligações e comunicações que cruzam a Internet [23]. Assim, entendemos que a Internet, embora sendo a principal rede telemática mundial, não representa todo o ciberespaço uma vez que este é algo mais vasto que pode surgir da relação do homem com outras tecnologias como o GPS, sensores biométricos ou câmaras de vigilância.

O ciberespaço cria mundos que, à primeira vista, parecem contíguos com o espaço geográfico, mas a verdade é que as leis da física têm pouco ou nenhum significado *online*. Isto ocorre porque o ciberespaço é puramente relacional, consistindo de diferentes media sendo todos eles artificiais, isto é, concebidos pelos seus criadores e muitas vezes até pelos próprios utilizadores [9]. Na realidade, o ciberespaço pode ser encarado como uma nova dimensão da sociedade, onde os fluxos de informação em rede redefinem toda uma

nova dinâmica social.

Conteúdo do Ciberespaço

O conteúdo do ciberespaço pode ser encarado numa perspectiva trinitária, considerando a existência de vários tipos de redes informacionais com características verdadeiramente distintas, tanto a nível de conteúdos como de facilidade de acesso: A *Surface Web*, a *Deep Web* e a *Dark Net*. A *Surface Web* é simplesmente aquilo a que todos nós acedemos no dia-a-dia, a *Deep Web* (também conhecida como *DeepNet*, *Invisible Web*, *Undernet* ou *Hidden Web*) refere-se ao conteúdo da *World Wide Web*[11] que não faz parte da *Surface Web*, ou seja, que não é indexável pelos motores de busca padronizados [1]. A *Dark Net* é uma rede anónima onde só se chega com o recurso a ferramentas específicas e que requerem já algum conhecimento técnico e, por isso mesmo, estará para sempre fora do alcance do utilizador comum.

***Surface Web* – A Internet das Massas**

No final de 2011, mais de um terço da população mundial (cerca de 2,3 mil milhões de pessoas) estava ligada à Internet [13] e aproximadamente 70% dos lares da OCDE tinham acesso a banda larga, a velocidades cada vez mais elevadas e a custos cada vez menores [20]. A esmagadora maioria dos utilizadores da Internet usa um motor de busca para obter informação e tomar decisões que podem ter impacto médico, financeiro, cultural ou político. No entanto, mais de 85% destes utilizadores não vai além da primeira página de resultados [15].

Os motores de busca generalistas e os directórios são fáceis de utilizar e respondem rapidamente às pesquisas informacionais. Por serem tão acessíveis e aparentemente todo-poderosos, é tentador limitar a pesquisa a uma simples entrada de duas ou três palavras e confiar na sorte. Estes motores de busca são recursos dirigidos a um público de massas, concebidos para fornecerem a toda a gente uma resposta para tudo [6]. No entanto, é importante ter em consideração que esta intenção de satisfazer virtualmente qualquer necessidade de informação é feita pagando um preço por isso. Os motores de busca generalista estão no mercado para ganhar dinheiro e este objectivo muitas vezes colide com o objectivo de executar pesquisas exaustivas e fornecer respostas completas [6]. Por outro lado, uma imensa multidão de cibernautas está apenas interessada nas redes sociais, no conteúdo descartável da piada do dia, no rumor do momento, no boato da semana. Esta é a face mais visível do ciberespaço contemporâneo, sendo de facto dirigido ao povo em geral.

***Deep Web* – A Internet Escondida**

A *Deep Web* é a parte da *Web* que o Google, Yahoo, Bing e outros não conseguem indexar e então ninguém sabe exactamente onde está [1]. Pensemos na *Web* como um oceano de conteúdos; o que está na superfície deste oceano é apenas aquilo para onde há ligações directas e que os motores de busca podem ver. Quaisquer outros conteúdos em partes mais profundas (protegido por autenticação ou simplesmente escondido) é-lhes inacessível. Há mais de dez anos que, utilizando esta analogia marítima num trabalho pioneiro ainda hoje muito citado [3], foi afirmado que as pesquisas na Internet podem ser comparadas ao arrastar de uma rede na superfície do oceano: embora se capture muita coisa na rede, há muito mais que se escapa nas profundezas da *Deep Web*.

A justificação para este facto é simples: a maior parte da informação da *Web* está enterrada em páginas que são geradas dinamicamente. Os motores de busca tradicionais criam os seus índices procurando a superfície da *Web*, mas descobrem apenas as páginas estáticas e para as quais existem ligações também estáticas e directas. Por outro lado, o conteúdo da *Deep Web* apenas pode ser alcançado como resposta a uma pesquisa específica e assim, essas páginas só existem se a sua criação for solicitada, ou seja, os recursos da *Deep Web* residem em bases de dados pesquisáveis que produzem resultados dinamicamente em resposta a pesquisas directas [3]. Os primeiros estudos sobre esta realidade apontam para estimativas díspares entre si. Em 2001, no estudo anteriormente referido, foi estimado que a *Deep Web* teria cerca de quinhentas vezes mais informação que a *Surface Web* [3], mas este número foi contestado [6] sendo a estimativa anterior reduzida para um número máximo de cinquenta vezes, considerando que muito do conteúdo referido no outro estudo é apenas especializado e não está exactamente escondido.

Actualmente, a *Web*, os *smartphones* e as redes sociais são ferramentas tecnológicas que fazem parte da experiência quotidiana do ciberespaço e da vida de muitos milhões de cibernautas. Mas, como já vimos, o Google, o Yahoo e o Bing apenas nos mostram menos de 20% do conteúdo da Internet, estando os restantes 80% escondidos [1] e fora do alcance do utilizador médio que jamais os procurará. Por outro lado, instituições académicas e outras organizações que não estão constrangidas pela procura do lucro, operam muitos dos recursos da *Deep Web* não sentindo a pressão de responder a tudo e todos. Assim, podem dar-se ao luxo de construir recursos de pesquisa exaustivos que permitem aos pesquisadores informados aprofundar extensivamente as suas investigações dentro de uma área específica, mantendo a informação sempre actualizada e organizada

[6]. Em contraste com a *Surface Web*, os recursos da *Deep Web* tendem a ser mais objectivos e frequentemente fornecem melhores resultados para quaisquer necessidades de informação.

Na realidade, ninguém sabe ao certo qual o volume exacto de informação contida actualmente na *Deep Web* uma vez que esta cresce a cada segundo que passa e a desproporção para a *Surface Web* não pára de aumentar. No entanto, pensamos ser seguro afirmar que hoje estaremos certamente para além de qualquer um dos números apontados em 2001 e assim o conteúdo actual da *Deep Web* é certamente muitas

centenas, senão mesmo milhares, de vezes superior ao da *Surface Web*. O advento das novas redes sociais, que incentivam à colocação de imensos conteúdos *online*, e a crescente tendência para a recolha de informação pessoal por diversos meios, levam a que o volume de dados existentes no ciberespaço não pare de crescer. Esta tendência agrava-se com a expansão da Internet a plataformas móveis e à exploração comercial das preferências dos cibernautas. Devido a este facto, ou seja, à existência de enormes quantidades de informação escondidas na *Deep Web*, esta tem atraído a atenção de diversas agências governamentais, desde espiões a militares [1]. Assim, a *Deep Web* constitui-se assim como uma área de pesquisa fora do alcance da população em geral, mas de grande interesse para um grupo mais restrito de utilizadores.

Dark Net – A Internet Anónima

O termo *Dark Net* refere-se a todos os conteúdos da Internet que podem apenas ser acedidos utilizando ferramentas de anonimato para identificar os endereços que não podem ser entendidos por um *browser* normal. A utilização destas redes é obrigatoriamente feita com recurso a um conjunto de ferramentas disponibilizado pelo projecto ToR (*The Onion Router*), mas há outras alternativas como o *Freenet Project* ou o I2P *(Invisible Internet Project)*, que têm também milhões de utilizadores. Aceder a estes *websites* sem utili-

zar um *browser* devidamente configurado para esse efeito, é completamente impossível e assim, a *Dark Net* pode ser entendida como uma subdivisão da *Deep Web* uma vez que o seu conteúdo também está escondido e fora do alcance dos motores de busca tradicionais [1]. À semelhança do que ocorreu com a própria Internet, a rede ToR foi originalmente concebida e implementada como parte de um projecto conjunto entre a *Defense Advanced Research Projects Agency* (DARPA) e os *Naval Research Laboratories* da marinha dos EUA, com o intuito de proteger as comunicações governamentais [1], mas há cerca de dez anos que está no domínio público e tem vindo a ser desenvolvida por voluntários de todo o mundo de tal forma que tem já dezenas de milhões de utilizadores.

A utilização do anonimato por si só não tem nada de ilegal e pode até ser um poderoso instrumento para iludir a censura governamental como ocorreu recentemente na Síria e no Egipto [1], onde os rebeldes se serviram destas ferramentas para comunicar de forma segura com o exterior. Mas, como ocorre com todas as novidades tecnológicas, o anonimato *online* atraiu imediatamente uma legião de criminosos que rapidamente se instalaram na *Dark Net* para vender todo o tipo de drogas, armas, pedofilia e todo o tipo de serviços, incluindo o aluguer de assassinos profissionais e de redes de computadores para lançar ataques informáticos. A *Dark Net* é também o local de encontro de muitas organizações terroristas e de crime organizado que se servem das características de privacidade da rede para se manterem em contacto de forma discreta e dissimulada. Pelas razões atrás apontadas, a *Dark Net* é uma crescente preocupação dos governos em todo o mundo, seja para a censurarem ou simplesmente para monitorizarem as actividades que decorrem nos cantos mais escuros do ciberespaço.

Em suma, o acesso ao ciberespaço é desigual na medida em que não existe uma homogeneidade na forma como estão organizados os seus conteúdos. O público em geral acede apenas à informação divulgada nas redes sociais e àquela derivada da primeira página de resultados dos motores de busca de referência, sendo tudo o resto acessível apenas a uma minoria mais esclarecida e interessada. Assim, podemos afirmar que o acesso contemporâneo ao ciberespaço é feito de forma trinitária: aos conteúdos mais banais acede o povo em geral, de forma fácil, natural e de acordo com as suas necessidades de consumo de informação mais ou menos trivial. Aos conteúdos da *Deep Web* já só acedem pesquisadores, estudantes e outros grupos de gente com interesses muito específicos e necessidades de informação rigorosa e detalhada. Por último, os conteúdos escondidos na *Dark Net* são alcançados por uma pequena elite de utilizadores, muitas vezes com interesses obscuros, o que torna este submundo virtual numa grande preocupação para os governos que se esforçam por, de alguma forma, controlá-lo e monitorizá-lo.

Tecnologia do Ciberespaço

O ciberespaço é hoje uma característica intrínseca da vida moderna e, à medida que a utilização global da Internet se expande, a tecnologia do ciberespaço tende a ficar totalmente embebida no nosso quotidiano. Consideramos ser também possível caracterizar a tecnologia do ciberespaço de forma trinitária uma vez que a sua utilização e o acesso à mesma se revestem de particularidades que lhe conferem esse mesmo carácter.

A tecnologia é popular

Indivíduos e comunidades de todo o mundo ligam-se, socializam e organizam-se através do ciberespaço. Entre 2000 e 2010, a utilização global da Internet passou dos 360 milhões de utilizadores para mais de 2,3 mil milhões [8]. Em Dezembro de 2011, o número estimado de ligações de banda larga sem fios na OCDE (667 milhões) era mais do dobro do número de ligações fixas (315 milhões) e a taxa de crescimento das assinaturas para serviços sem fios continua a aumentar. Simultaneamente, enquanto a velocidade de acesso em banda larga aumenta, os preços desses serviços diminuem [20].

Por outro lado, o número de subscrições de telemóvel a nível mundial duplicou desde 2005 e, no mesmo período, triplicou nos países fora da OCDE [20]. Assim, no final de 2011, havia cento e cinco países no mundo com mais assinaturas de telemóvel do que cidadãos [13]. A crescente proliferação dos *smartphones* e *tablet PC* permite aceder a tudo em todo o lado e, por outro lado, o preço dos serviços de telemática desceu, em média, 30% entre 2008 e 2011 [13]. Estas tendências conferem às novas tecnologias de comunicação um carácter verdadeiramente popular.

A tecnologia é militarmente importante

As modernas forças armadas estão cada vez mais dependentes de recursos informacionais e do ciberespaço, especialmente quando são projectadas para os antípodas. Estes recursos são utilizados numa variada panóplia de sistemas desde o comando e controlo, à logística, passando pela vigilância por satélite, pela geolocalização ou ainda pelo fluxo bidireccional de informação desde o nível táctico ao nível estratégico [24].

Os militares norte-americanos utilizam também a *Dark Net* para que os seus agentes infiltrados no terreno possam comunicar as recolhas de informação efectuadas [1]. Na realidade, existe mesmo um departamento da marinha dos EUA que utiliza esta rede abertamente para a recolha de informação e uma das suas equipas utilizou recentemente o sistema ToR no Médio Oriente [1]. Ao longo das últimas duas décadas, muitos especialistas em segurança têm afirmado que o ciberespaço é o novo domínio da guerra. Mais importante ainda, a capacidade para aceder e operar no ciberespaço é de declarado interesse para a soberania e prosperidade dos EUA [2].

Em 2011, o Departamento de Defesa norte-americano (DoD) declarou oficialmente a sua dependência do ciberespaço para o seu funcionamento efectivo, referindo explicitamente que opera mais de quinze mil redes e sete milhões de dispositivos de computação, distribuídos por centenas de instalações em dezenas de países em todo o mundo. Nesse mesmo documento [8], o DoD assume que utiliza o ciberespaço para a inteligência militar e operações comerciais, incluindo as movimentações de pessoal e material e o comando e controlo do espectro completo das suas operações militares. É assim inequívoco afirmar que as novas tecnologias são de grande relevância militar e que as forças armadas dos países mais desenvolvidos estão atentas a esta realidade.

A tecnologia é financiada pelo governo

A Internet, tal como a conhecemos hoje, nasceu de um projecto governamental norte-americano e foi durante largos anos controlada por órgãos do governo dos EUA. Mais tarde, a expansão a instituições de ensino, financeiras e ao uso doméstico levaram a que a moderna Internet seja hoje regulada por organizações não-governamentais. No entanto, os governos ocidentais continuam apostados na tecnologia como forma de progresso e os decisores políticos estão cada vez mais empenhados no desenvolvimento da Internet e das tecnologias da informação.

Em 2011, os governos da OCDE indicaram que as suas prioridades continuariam a ser a expansão da banda larga e a continuação da transferência de serviços governamentais para o ciberespaço [20]. Numa altura em que o orçamento federal da defesa dos EUA sofre cortes significativos, o financiamento do ciberespaço continua a subir [2]. A estratégia apresentada em 2011[14], estima que um quarto das despesas federais com tecnologias da informação, cerca de vinte mil milhões de dólares, podem ser migradas para a "nuvem"[2], aproveitando este desenvolvimento tecnológico.

Por outro lado, o interesse nas vastas quantidades de informação existentes na *Deep Web* levam os governos a financiar novas ferramentas para monitorizar, explorar ou mesmo bloquear o acesso a estas redes [1] [8], tendo em conta que, por exemplo, a migração para a *cloud* é uma realidade exequível mas que carece de redobradas medidas de segurança [19]. Ou seja, o nível de investimento em tecnologias militares e o grau de aproveitamento de tecnologias civis em prol do esforço militar são aspectos sobre os quais cabe ao governo decidir.

Utilização do Ciberespaço

O ciberespaço envolve-nos de forma silenciosa e omnipresente. O crescimento explosivo da Internet trouxe consigo uma série de efeitos sociais e culturais que têm moldado todo o panorama mediático e cujos efeitos são cada vez mais visíveis em todos os quadrantes da comunicação. O surgimento desta entidade, que integra o nosso quotidiano, permitiu que a informação se dissemine de forma global. Os actores políticos, empresariais e religiosos, estão hoje plenamente cientes desta realidade e a propaganda está a ser devidamente adaptada, sendo cada vez mais simplificada de modo a alcançar e ter impacto numa audiência mais alargada.

O ciberespaço é veículo de ódios violentos

Este assunto já foi alvo de reflexão de vários autores que alertaram para diversos fenómenos emergentes como por exemplo o facto de as sociedades secretas e organizações marginais com presença na Internet serem agora capazes de atrair novos membros numa vasta área geográfica. A sua propaganda e a informação sobre as suas teorias da conspiração, crenças e práticas culturas são assim facilmente transmitidas [18]. A Internet é utilizada por diversas organizações terroristas como uma ferramenta de radicalização e recrutamento, como método para a distribuição de propaganda em massa, como meio de comunicação e como até como método de treino [25].

Por outro lado, a Internet permite o luxo de evitar o contacto físico com outros elementos do grupo mas, ainda assim, permitir recrutar novos membros sem deixar o conforto doméstico. Ou seja, o uso desta propaganda tornou-se a norma entre os grupos terroristas [17]. Esta problemática tem sido abordada nos últimos anos com especial realce para o impacto que os desenvolvimentos tecnológicos têm tido nas relações internacionais e na velocidade a que essas mudanças ocorrem [21]. Assim, é hoje inegável que quase todas as organizações minoritárias e regionais da Europa reclamaram para si um pouco de ciberespaço com o intuito de darem expressão às suas agendas políticas, reclamações de independência ou apenas para repetir e amplificar conteúdos de outros media [23].

Além disso, as organizações terroristas, ou extremistas individuais, exploram a Internet como meio para a difusão de ataques supostos bem-sucedidos, imagens de pretensos

mártires e discussão de ideologia [25]. Cada vez mais, os activistas modernos podem exprimir as suas opiniões, e até ameaças, recorrendo a técnicas multimédia que produzem um efeito mais abrangente que aquele conseguido pela tradicional propaganda oral [21]. Os novos meios de comunicação, e em particular a Internet, permitem que os grupos marginais transcendam o monopólio dos media oficiais embebidos na estrutura estatal vestefaliana, ou seja, as minorias nacionais estão particularmente bem servidas pelo advento da Internet e do ciberespaço [23].

O ciberespaço é transnacional e imprevisível

O ciberespaço e as diversas redes nele contidas proporcionam um elevado grau de anonimato e isto implica a ausência de barreiras, de fronteiras e de autoridade o que permite que um atacante possa, virtualmente sem quaisquer consequências, atacar qualquer pessoa ou qualquer coisa em qualquer ponto do globo [17]. Além disso, se encararmos o ciberespaço como geografia, torna-se imediatamente evidente que os estados-nação estão muito mal representados no espaço virtual por oposição ao espaço real [23]. Com tantos conteúdos e utilizadores ligados, o ciberespaço há já muito tempo que se tornou uma entidade confusa, difícil de monitorizar [9] e onde pode ser muito difícil navegar. Por um lado, a natureza descentralizada da Internet como meio de comunicação e a correspondente dificuldade em responder às ameaças emergentes, favorecem a natureza distribuída das organizações e operações terroristas [25] e, por outro lado, as operações no ciberespaço são, não só desordenadas e imprevisíveis, mas também mais difíceis de caracterizar rigorosamente que as tradicionais operações cinéticas o que pode ter sérias implicações no planeamento e execução de tais operações [2].

Sem qualquer consideração por opções económicas, religiosas, raciais ou políticas, na aldeia virtual global, os fusos horários são agora mais importantes do que as fronteiras [21], num mundo que está permanentemente ligado e onde a qualquer momento podem ocorrer os mais inesperados fenómenos de todo o tipo. A Internet está dramaticamente a redefinir a natureza das relações entre nações e a desafiar a sua soberania cultural ao criar um sentimento de ausência de fronteiras. Com a criação de comunidades virtuais baseadas em factores étnicos, linguísticos ou outro tipo de afinidades, esbate-se a prevalência das fronteiras nacionais na definição da identidade cultural [23].

O ciberespaço é realmente uma nova dimensão, sem fronteiras políticas, universal e potencialmente muito perigoso. Neste novo espaço virtual, o território é irrelevante o que significa que é inevitável uma alteração radical do tradicional modelo de soberania e jurisdição que tem vigorado nas últimas centenas de anos [12]. O labirinto informacional e estrutural da Internet permite aos potenciais atacantes um elevado grau de anonimato e estes podem encaminhar os seus ataques através de países com as quais o alvo tem fracos laços diplomáticos e nenhuma cooperação policial. O resultado é que as investigações acabarão num beco sem saída, levando apenas à descoberta de mais violações de segurança sem que isso revele quaisquer pistas concretas.

O ciberespaço é racionalizado pelos governos

Para muitos governos, a *Deep Web* é um inimigo a abater visto dar voz e expressão a dissidentes, permitindo-lhes divulgar as realidades que interessa manter escondidas. É esta a razão pela qual estão a adquirir tecnologia para monitorizar e controlar o ciberespaço, bloqueando o acesso às redes como a ToR que, nestes países, é uma verdadeira "rede da liberdade". É o que está a acontecer, por exemplo, na Síria, Irão, Etiópia e China, onde os governos querem negar ao seu próprio povo o livre acesso à informação e o direito a falar abertamente dos seus problemas [1].

Por outro lado, multiplicam-se as iniciativas governamentais para exercer algum tipo de controlo e regulamentação sobre o ciberespaço, numa tentativa de prevenção da crescente vaga de ciberameaças de diversos tipos. A OSCE estabeleceu o *Action Against Terrorism Unit*, a OTAN criou o *Cooperative Cyber Defense Center of Excellence* na Estónia e a União Europeia lançou a *Critical Information Infrastructure Protection Initiative* [12]. Noutro âmbito, citamos, apenas a título de exemplo, a ordem executiva 13618 assinada em Julho de 2012 pelo presidente Barack Obama que pode dar ao governo dos EUA controlo sobre a Internet. Com o sugestivo título de *Assignment of National Security and Emergency Preparedness Communications Functions*, esta ordem foi concebida para permitir que algumas agências governamentais possam assumir o controlo total das telecomunicações e da *Web* em caso de catástrofe natural ou emergência de segurança nacional [22].

Se muitos governos apostam na Internet como meio de desenvolvimento e democratização, outros há que a censuram e bloqueiam de forma ostensiva, demonizando a sua pretensa influência maléfica sobre o povo. Na realidade, muitos governos a nível mundial têm, embora muitas vezes tardiamente, reconhecido que a Internet e o ciberespaço fornecem aos seus opositores as mais modernas ferramentas para os criticarem e atacarem das mais diversas formas. Consequentemente, estão a ripostar, tentando repor a sua influência e tentando evitar que projectos supostamente conotados com determinadas minorias possam atingir identidade ciberespacial e crescer em escala e âmbito [23] [12].

O carácter trinitário da conflitualidade cibernética

Uma ameaça cibernética pode ser vagamente definida como uma tentativa consciente de obter acesso não autorizado a um sistema de computadores para extrair ou manipular dados ou violar a confidencialidade, autenticidade, integridade ou disponibilidade de dados dentro do sistema. Embora existam inúmeras formas de organizar e categorizar estas actividades e se possam encontrar diversas opiniões diferentes sobre o assunto, no âmbito deste trabalho iremos apenas considerar a existência de três grandes tipos de ciberameaças: o cibercrime, a ciberguerra e o ciberterrorismo.

Cibercrime

Genericamente, o cibercrime é aquele que é cometido com recurso a tecnologias de informação. Esta definição, embora possa parecer demasiado vaga, engloba os crimes cometidos utilizando a Internet, os crimes digitais e os que envolvem as redes de telecomunicações. Embora as actividades de cibercrime possam, por vezes, coexistir com o ciberterrorismo, na sua essência são coisas muito diferentes porque os criminosos procuram principalmente atacar sistemas em busca de alguma forma de lucro financeiro, enquanto o terrorismo tem sempre motivações políticas e ideológicas.

Phishing

O *phishing* consiste basicamente em levar a que os utilizadores insiram dados pessoais num *site* falso, cuja aparência é quase idêntica à do legítimo. O esquema é normalmente realizado através de correio electrónico e é um bom exemplo de uma técnica de engenharia social utilizada na tentativa de adquirir informações pessoais, como nomes de utilizador, senhas ou informações de cartão de crédito. O termo é uma variante de pesca (*fishing*), provavelmente influenciado pelo *phreaking* (*phone freaking*), e refere-se ao "isco" utilizado na esperança de que a potencial vítima o "morda" ao receber comunicações que pretendem ser de populares *sites* sociais, *sites* de leilões, processadores de pagamento online ou administradores de TI. Ao clicar em ligações para *sites* que estão infectadas com *malware*[3] ou ao abrir um anexo malicioso, as suas informações financeiras e senhas podem ser roubadas.

O *smishing* é uma das variantes do *phishing* que é executada através da utilização de técnicas de engenharia social através de SMS (*Short Message Service*), a tecnologia utilizada para mensagens de texto em telefones celulares. Daí o nome, derivado de "SMs phISHING". O *vishing* é uma prática criminosa, também derivada do *fishing*, recorrendo ao uso de engenharia social sobre o sistema de telefonia, e que tem sido facilitada pelo VoIP (Voz sobre IP) explorando a confiança do público em geral nos serviços de telefonia fixa. O termo é uma combinação de *voice* (voz) e *phishing*.

Spamming

Spam é o uso de sistemas electrónicos de mensagens para o envio indiscriminado e em massa de mensagens não solicitadas. Indivíduos ou organizações (chamados *spammers*) distribuem mensagens de correio electrónico não solicitadas com informações ocultas ou falsas, principalmente de publicidade, a fim de vender produtos, mas muitas vezes também espalhando várias formas *malware* e realizando vários esquemas de *phishing*. O termo refere-se geralmente ao *spam* de correio electrónico mas também é aplicado a práticas semelhantes em quase todos os outros meios de comunicação, como mensagens

instantâneas, grupos da *Usenet*, motores de busca da Web, blogs, etc. O nome vem de uma paródia dos Monty Python em que o spam (*spiced ham*) está incluído em quase todos os pratos.

Botnets

As *botnets* (*roBOT NETworks*) são grupos de computadores, ligados uns aos outros através da Internet de forma involuntária, que podem ser controlados remotamente para desempenhar diversas tarefas tais como enviar *spam mail*, executar ataques DDoS (*Distributed Denial of Service*) ou ainda recolher informação pessoal. As *botnets* são tipicamente criadas através da infecção de um virus informático ou da instalação de *malware*. Este *software* pode assumir diversas formas, mas as mais vulgares são aquelas normalmente conhecidas como cavalos de Tróia (em referência ao famoso episódio da Ilíada porque normalmente se escondem dentro de outro software) e cópias ilegais de programas tirados de *sites* da Internet que o fazem intencionalmente. Ao instalar este *software* o utilizador está inadvertidamente a instalar também o cavalo de Tróia e corre o risco de, sem o saber, estar a disponibilizar o seu computador como mais um zombie pronto a integrar uma *botnet* às ordens de um qualquer criminoso que o pretende usar com fins obscuros.

Spyware

Trata-se de *software* malicioso instalado num sistema, através do engodo dos utilizadores, para recolher informações sem o seu conhecimento. O *spyware* pode entrar no sistema no meio de outro software legítimo ou escondido usando um cavalo de Tróia que o torna difícil de detectar. Este tipo de *software* também pode ser intencionalmente instalado pelo administrador de computadores empresariais, a fim de observar o comportamento dos utilizadores, mas nesse caso é considerado software de monitorização.

Pedofilia

Embora muito raramente associadas ao cibercrime, as redes de partilha de pedofilia cresceram exponencialmente com a difusão da Internet. O que antes era limitado a grupos muito secretos e geograficamente confinados, gozou durante alguns anos de novos e grandes meios de recolha de novos maníacos e foi um negócio próspero para muita gente sem escrúpulos. Apesar de ser uma prática ilegalizada e condenada globalmente, está longe de estar erradicada e nos últimos anos têm sido expostas diversas redes deste tipo, algumas delas a operar na *Dark Net* [1].

Ainda que a lista anterior não seja exaustiva e possa ser controversa, o seu objectivo é

apenas ilustrar a variedade da criminalidade existente no ciberespaço contemporâneo. Embora seja verdade que há também registo de ataques a grandes instituições financeiras de onde desaparecem largas somas de dinheiro, também é verdade que esses episódios são esporádicos, enquanto os ataques supracitados ocorrem diariamente e afectam milhões de incautos cibernautas. Ou seja, pensamos ser legítimo afirmar que, de uma forma genérica, o cibercrime afecta o primeiro pilar da trindade clausewitziana, ou seja, o povo em geral.

Ciberguerra

A ciberguerra pode ser encarada como o conjunto de acções tomadas por uma nação ou estado contra sistemas de computador de outra nação com o objectivo de causar danos ou interrupção de serviços, transformando assim o ciberespaço no novo domínio da guerra. O ciberespaço é um campo aberto para os estrategas militares e alguns países ocidentais estão já oficialmente a avançar para lá da guerra clássica envolvendo força física [8]. Mas há um grande debate centrado em como aplicar o conjunto existente de leis internacionais sobre a guerra e como proteger os civis em caso de um conflito cibernético alargado [12].

Nos últimos anos têm sido recorrentes os ataques de ciberespionagem contra diversas empresas, resultando no roubo de muita informação classificada. Embora se possa considerar que se trata de simples espionagem industrial, ou seja, uma actividade criminosa, a verdade é que a esmagadora maioria desses ataques são realizados contra indústrias de defesa. Por isso, consideramos que estes ataques podem também ser enquadrados no âmbito geral da ciberguerra uma vez que visam essencialmente o roubo de tecnologia com interesse militar.

Consequentemente, os programas de guerra cibernética são projectos patrocinados pelos governos para desenvolver capacidades com a perspectiva futura de causar danos generalizados a infra-estruturas críticas. Recentemente, o mundo soube da disseminação do Stuxnet[4], a primeira ciberarma realmente desenvolvida para ser usada contra uma nação estrangeira. Esta arma cibernética é um bom exemplo da dificuldade em estabelecer com rigor quando é que uma acção deste tipo atinge o patamar da guerra porque no ciberespaço pode ser quase impossível identificar os inimigos. Na ciberguerra não há imagens de satélite de veículos blindados nem de movimentos de tropas e muito pouco pode ser feito para provar se uma nação lançou ou não um ataque.

Várias nações estão agora a trabalhar agressivamente no desenvolvimento de doutrina da guerra de informação e de programas e recursos que incluem armas cibernéticas reais [8] [2] [24]. Estas novas armas cibernéticas podem ter um impacto significativo ao perturbarem os fornecimentos, as comunicações e infra-estruturas económicas que sustentam a vida quotidiana dos cidadãos em todo o país alvo. Além disso, os serviços de inteligência militar utilizam ferramentas cibernéticas como parte das suas actividades de colecta de informações e espionagem. Assim, sendo uma actividade em que, ainda que

dissimuladamente, um estado ataca outro estado por meios informáticos, e onde a maior parte dos ataques de espionagem são dirigidos contra indústrias militares, podemos afirmar que está em causa o segundo pilar da trindade clausewitziana, ou seja, os militares.

Ciberterrorismo

O ciberterrorismo tornou-se uma das ameaças mais significativas para a segurança nacional e internacional dos estados modernos, e os ciberataques ocorrem com cada vez maior frequência [12]. Sendo um assunto politica e emocionalmente carregado, nunca foi possível chegar a um consenso internacional sobre o desenvolvimento de uma definição globalmente aceite do termo "terrorismo". Tentando evitar essa polémica, podemos simplesmente, de forma genérica, considerar que o terrorismo consiste na realização de actos criminosos destinados ou planeados para provocar um estado de terror no público em geral, num grupo de pessoas ou pessoas particulares para fins políticos.

Tendo isto em consideração, como podemos definir ciberterrorismo? É, obviamente, um termo muito controverso, com muitas definições possíveis, dependendo do âmbito das acções realizadas. Tentando evitar todo o debate em torno da motivação, objectivos e métodos envolvidos, consideramos que o ciberterrorismo é a utilização da Internet e das tecnologias de informações, com motivações ideológicas, para organizar e executar ataques contra as redes de computadores, sistemas e infra-estruturas de telecomunicações. Apesar da existência de uma grande carga de subjectividade acerca daquilo que se pode classificar exactamente como ciberterrorismo, é lógico assumir que o conceito tem obrigatoriamente que conter sistemas de computador, quer como alvos ou como ferramentas. Assim, o ciberterrorismo pode ser estudado no âmbito de uma convergência do terrorismo e do ciberespaço. Para ser considerado como terrorismo, um ataque deve visar a produção de violência contra pessoas ou bens, ou pelo menos causar danos suficientes para gerar medo. Além disso, para se qualificar como "ciber" tem que implicar ataques e ameaças contra computadores, redes, ou a informação que eles armazenam.

Pensamos portanto ser legítimo afirmar que o ciberterrorismo é o ataque, intencional e politicamente motivado, lançado contra sistemas de informação e que potencialmente pode resultar em violência contra alvos não militares. As ameaças ao sistema financeiro internacional constituem uma das maiores ameaças do ciberterrorismo [12], visto que uma acção desse tipo, bem sucedida, terá um impacto político global. Por outro lado, um terrorista não precisa ter explosivos poderosos, apenas acesso a um computador e à Internet. Mais importante ainda, a Internet oferece aos ciberterroristas um novo alvo, maior do que qualquer um dos tradicionais objectivos que poderiam alguma vez atingir com um ataque físico directo. Teoricamente, sem necessidade de construir uma bomba ou de se sacrificarem, os ciberterroristas podem afectar a infra-estrutura crítica de uma nação, criar o caos na economia global e incutir o pânico em milhões de pessoas [12]. Assim, embora os alvos do ciberterrorismo possam ser diversificados, sendo uma

actividade intrinsecamente conduzida e planeada com objectivos políticos, parece-nos que está inequivocamente em causa o terceiro pilar da trindade, ou seja, o governo.

Conclusões

Muitos dos assuntos abordados por Clausewitz estão hoje obsoletos em face dos desenvolvimentos tecnológicos mas, de qualquer forma, a sua trindade permanece como um edifício conceptual eterno e que continua a servir para o estudo da moderna conflitualidade, seja qual for o contexto em que esta decorra. O ciberespaço é a nova fronteira onde se digladiam os contendores das modernas batalhas de propaganda e contrapropaganda em duelos cibernéticos que escapam ao controlo das autoridades reguladoras e afectam a percepção da realidade de boa parte dos incautos cibernautas, tentando orientá-los para o apoio às suas causas, sejam elas quais forem. Sucessivas campanhas de desinformação tentam criar, e manter acesos, os mais diversos focos de ódios primários assentes nas mais variadas causas, sendo este um dos aspectos da trindade que mais facilmente pode ser identificado.

Por outro lado, apesar de todos os esforços feitos no sentido incrementar a segurança dos sistemas de informação, o ciberespaço tornar-se-á um ambiente cada vez mais hostil visto que através dele podem ser lançados ataques perfeitamente anónimos e dirigidos a alvos altamente remuneradores. O acaso, tal como Clausewitz o definiu, não se refere apenas às ocorrências aleatórias mas também ao facto de um conflito armado ser, desde o nível táctico ao nível estratégico, uma avaliação de probabilidades e tomada de decisões. A ênfase por ele colocada na imprevisibilidade da guerra, devido às múltiplas variáveis em causa, prova a imensa importância por si atribuída à adaptabilidade. No mundo moderno em rápida mutação, impulsionado pelos constantes desenvolvimentos tecnológicos e pela instabilidade das relações internacionais, esta componente da trindade mantém a sua actualidade e muitos estados enfrentam hoje a ameaça real de derrota num ciber conflito sem sequer conhecerem a identidade do inimigo.

As guerras cibernéticas continuam a ser clausewitzianas na sua essência, envolvendo os mesmos grupos sociais da trindade, embora com outras roupagens uma vez que, por exemplo, os interesses económicos se confundem frequentemente com os da indústria militar. De forma semelhante, também os governos já não são sempre representados pela clássica liderança política de um estado uma vez que boa parte da conflitualidade moderna decorre entre actores do sistema internacional que não são estados. Quanto ao povo, relacionado com o primeiro pilar nas suas diversas incarnações, pode ser o alvo preferencial com o inimigo a visar os seus bens financeiros ou a utilizar a propaganda para o manipular.

No entanto, apesar de todas estas diferenças derivadas da evolução mundial, a moderna conflitualidade cibernética retém as características trinitárias intrínsecas a qualquer guerra, tal como Carl von Clausewitz teorizou, bem antes do advento da qualquer uma destas modernas tecnologias. A sua concepção da guerra, a sua trindade e o seu

entendimento das relações entre a política e a guerra, são válidas enquanto os estados, os cartéis da droga ou os grupos terroristas se envolverem em conflitos, ou seja, as suas concepções sobre a natureza da guerra são absolutamente intemporais.

Bibliografia

[1] Amores, R. and Paganini, P. 2012. *The Deep Dark Web*. CreateSpace Independent Publishing Platform.

[2] Bartholomees Jr., J.B. ed. 2012. *U.S. Army War College Guide to National Security Issues, Volume I: Theory of War and Strategy*. Strategic Studies Institute.

[3] Bergman, M.K. 2001. The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing*. 7, (2001).

[4] Bernard, C.S. 1999. Clausewitz in the 21st Century. *The Army Doctrine and Training Bulletin*. 2, (1999).

[5] Brown, R. 2002. Clausewitz in the Age of Al-Jazeera. *Rethinking the Military-Media-Relationship, Paper prepared for the APSA Political Communication Division Workshop, Harvard/Ma* (2002).

[6] Chris Sherman, G.P. 2001. *The Invisible Web: Uncovering Information Sources Search Engines Can't See*. CyberAge.

[7] Clausewitz, C. von 2008. *On War*. AuthorHouse.

[8] DoD 2011. *DoD Strategy for Operating in Cyberspace*. U.S. Department of Defense.

[9] Dodge, M. and Kitchin, R. 2001. *Atlas of Cyberspace*. Addison-Wesley.

[10] Echevarria II, A.J. 2005. *Fourth-generation war and other myths*. DTIC Document.

[11] Echevarria II, A.J. 1996. War, Politics, and RMA-The Legacy of Clausewitz. *Joint Force Quarterly*. (1996), 76–80.

[12] Gable, K.A. 2010. Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. *Vanderbilt Journal of Transnational Law*. 43, (2010), 57–118.

[13] ITU 2012. *Measuring the Information Society, 2012*. International Telecommunication Union.

[14] Kundra, V. 2011. *Federal Cloud Computing Strategy*. White House, Chief

Information Officers Council.

[15] Metaxas, P.T. and DeStefano, J. 2005. Web spam, propaganda and trust. *the 1st International Workshop on Adversarial Information Retrieval on the Web (AIRWeb)* (2005).

[16] Miller, S. 2012. Are Clausewitz and Sun Tzu Still Relevant in Contemporary Conflicts? e-International Relations.

[17] Minei, E. and Matusitz, J. 2012. Cyberspace as a new arena for terroristic propaganda: an updated examination. *Poiesis & Praxis: International Journal of Ethics of Science and Technology Assessment*. 8, (2012), 1–5.

[18] Nayar, P.K. 2010. *An Introduction to New Media and Cybercultures*. John Wiley & Sons.

[19] NSTAC 2012. *Report to the President on Cloud Computing*. National Security Telecommunications Advisory Committee.

[20] OECD 2012. *OECD Internet Economy Outlook 2012*. OECD Publishing.

[21] Otte, J.T. 2009. *Cyberspace and Propaganda: Threats and Opportunities of International Mass Media, Embedded Journalism, and Propaganda Carried Out by None-state Actors on the Internet, Social Networks and Blogs in the Current Israeli-Palestinian Conflict*. Hammer, Patrick, Tanja Hammer, Matthias Knoop, Julius Mittenzwei, Georg Steinbach u. Michael Teltscher. GRIN Verlag GbR.

[22] Reese, S. 2012. *National Security and Emergency Preparedness Communications: A Summary of Executive Order 13618*. Congressional Research Service.

[23] Saunders, R.A. 2011. *Ethnopolitics in Cyberspace: The Internet, Minority Nationalism, and the Web of Identity*. Lexington Books.

[24] Sharma, A. 2010. Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis*. 34, (2010), 62–73.

[25] Theohary, C.A. and Rollins, J. 2011. *Terrorist Use of the Internet: Information Operations in Cyberspace*. Congressional Research Service.

[26] Weaver, D. 2011. Leopards Don’t Change Their Spots: Clausewitz in the 21st Century. e-International Relations.

[1] A World Wide Web (mais conhecida pela famosa sigla WWW ou simplesmente como a web) é um sistema de documentos disponíveis na Internet que, hoje em dia, permite o acesso a um vasto conjunto de informação multimédia. A ideia básica por trás da web é a navegação em hipertexto, ou seja, os conteúdos podem ser lidos de forma não sequencial. O acesso a esta informação é feito através de um programa de computador chamado navegador (*browser*) em que o utilizador escolhe o que vai ler através do acesso feito pelas diferentes ligações entre as páginas (*links*). É a este processo que vulgarmente se chama "surfar na web", ou "navegar na net".

[2] A expressão "computação na nuvem" (*cloud computing*) refere-se a um novo conceito de consumo de tecnologia através da Internet que assenta na lógica da partilha de recursos através da rede. Ou seja, o *cloud computing* consiste essencialmente em tirar partido das capacidades de armazenamento e processamento de computadores e servidores partilhados e interligados por meio da Internet para ter acesso a um conjunto variado de serviços, disponíveis a qualquer momento e em qualquer lugar, independentemente da plataforma de acesso, com a mesma facilidade de tê-los instalados nos computadores pessoais.

[3] O termo *malware* refere-se genericamente a código informático malicioso (*malicious software)* onde se incluem ameaças de vários tipos que se propagam de diversas formas, como por exemplo os vírus, os worms, o *spyware*, os cavalos de Tróia, etc. Entre muitas outras coisas, o *malware* tenta explorar as vulnerabilidades existentes nos sistemas, abrindo portas de entrada que permitem a um intruso ter acesso a informação privada, ou recolhe e envia directamente essa informação.

[4] O Stuxnet é um *worm* de computador concebido especificamente para atingir as unidades de enriquecimento de urânio do Irão, em Natanz. O *worm* é incomum visto que, apesar de se propagar através de computadores com sistema operativo Windows, a sua carga útil é direccionada apenas para uma configuração específica de sistemas de supervisão e aquisição de dados (*Supervisory Control and Data Acquisition* – SCADA), ou seja, exactamente aquilo que o Irão tem nas suas centrifugadoras. Na altura da sua descoberta, o Stuxnet é considerado o mais avançado *malware* já estudado e aumenta significativamente o nível da ciberguerra. Actualmente já é claro que se tratou de um ataque cibernético real sobre as instalações nucleares do Irão com a maioria dos especialistas a acreditar que Israel está por trás disso, com a ajuda dos EUA. O Stuxnet é a primeira arma cibernética de nível militar do mundo conhecida publicamente, capaz de destruir máquinas, e o ataque retarda significativamente o programa iraniano de enriquecimento de urânio ao danificar cerca de mil centrifugadoras.