OBSERVARE
Universidade Autónoma de Lisboa

e-ISSN: 1647-7251
Vol. 11, Nº. 1 (Maio-Outubro 2020), pp. 19-31

COMBATER O CIBERCRIME COMO PRÉ-REQUISITO PARA O DESENVOLVIMENTO DA SOCIEDADE DIGITAL

Olga A. Klymenko
ms-kl18@ukr.net
Doutorada em Direito. Chefe do Departamento do Centro Interinstitucional de Pesquisa sobre Problemas de Combate ao Crime Organizado no Conselho Nacional de Segurança e Defesa da Ucrânia (de 2017 a 2019), Kiev (Ucrânia).

Mykhaylo V. Gutsalyuk
mvgutsalyuk@ukr.net
Doutorado em Direito, Professor Associado. Pesquisador-chefe do Centro Interinstitucional de Pesquisa sobre Problemas de Combate ao Crime Organizado no Conselho Nacional de Segurança e Defesa da Ucrânia, Kiev (Ucrânia).

Andrii V. Savchenko
savchenkoav@ukr.net
Doutorado em Direito (LLD). Professor do Departamento de Direito Penal da Academia Nacional de Assuntos Internos, Kiev (Ucrânia).

Resumo

O artigo trata das questões de segurança cibernética e crime cibernético na sociedade digital. São propostas áreas para melhorar a cooperação internacional para garantir a segurança da Internet.

A sociedade digitalizada está a ser implementada em todo o mundo a uma taxa elevada e oferece benefícios significativos para o desenvolvimento da sociedade como um todo e dos seus componentes individuais. Ao mesmo tempo, um fator que afeta negativamente esse desenvolvimento é o cibercrime. O artigo explora o estado atual e as principais tendências do crime cibernético, incluindo as suas formas organizadas.

São propostas medidas legislativas e organizacionais para combater o cibercrime, salientando o papel principal da cooperação internacional, incluindo o rápido intercâmbio de dados eletrónicos para detetar e investigar o cibercrime.

Palavras chave

Cibercrime; cibersegurança; cooperação internacional; sociedade digital; contração.

Como citar este artigo

Klymenko, Olga A.; Gutsaliuk, Mykhailo V.; Savchenko, Andrii V. (2020). "Combater o cibercrime como pré-requisito para o desenvolvimento da sociedade digital". *JANUS.NET e-journal of International Relations*, Vol. 11, N.º 1, Maio-Outubro 2020. Consultado [em linha] em data da última consulta, https://doi.org/10.26619/1647-7251.11.1.2

Artigo recebido em 12 de Novembro de 2019 e aceite para publicação a 26 de Março de 2020

COMBATER O CIBERCRIME COMO PRÉ-REQUISITO PARA O DESENVOLVIMENTO DA SOCIEDADE DIGITAL

Olga A. Klymenko
Mykhaylo V. Gutsalyuk
Andrii V. Savchenko

Descrição do problema

Um dos sinais da sociedade digital moderna é o rápido desenvolvimento das tecnologias da informação e a disseminação da Internet, que estão a ser introduzidos em todas as esferas da vida. O primeiro site da história foi criado em 1991 e hoje existem mais de 1,8 biliões de sites no mundo. Se em 2015 o número de utilizadores da Internet era de cerca de 2 biliões, em 2019 eles já ultrapassavam os 4 biliões (Estatísticas ao vivo na Internet, 2019).

O primeiro programa da Europa Digital, proposto em junho de 2018, investirá em cinco principais setores digitais: computadores de alto desempenho, inteligência artificial, segurança cibernética e confiança, habilidades digitais avançadas, e garantir o amplo uso e implantação de tecnologias digitais na economia e na sociedade, afim de fortalecer a liderança tecnológica industrial europeia (Orçamento da UE, 2018).

Ao mesmo tempo, com o desenvolvimento da tecnologia informática, surgiu uma nova forma de atividade criminosa – o cibercrime, que hoje domina o ambiente de redes de computadores e dispositivos móveis. O anonimato das redes globais de informação, a velocidade da transferência de informações possibilita o uso dessas vantagens, não apenas no desenvolvimento da sociedade de informação, mas também pela prática de atos ilícitos. Isso também é facilitado pelo facto das tecnologias de informação e comunicação estarem a ser introduzidas e desenvolverem-se muito mais rapidamente do que os legisladores e as agências de aplicação da lei podem reagir. Portanto, o desenvolvimento sustentável de uma sociedade digital só é possível se o crime cibernético for combatido ativamente, incluindo as suas formas organizadas.

Os crimes cibernéticos, contrariamente aos tradicionais, são caracterizados pelo facto de serem cometidos usando computadores e redes de dados, incluindo a Internet global. Como resultado, esses crimes podem ser de natureza transfronteiriça e perpetrados por grupos interestaduais criminosos organizados. Outra característica é que a evidência de tais crimes está contida em dispositivos eletrónicos (evidência eletrónica ou digital) e tem a capacidade de ser rapidamente modificada ou mesmo destruída.

Depois da Organização Mundial da Saúde ter reconhecido o coronavírus como uma pandemia, muitas organizações em todo o mundo começaram a introduzir métodos remotos de trabalho nas suas unidades, incluindo organizações como o Congresso dos EUA, o Pentágono, a NASA. Ao mesmo tempo, o tráfego da Internet aumentou significativamente. Por exemplo, o tráfego de conferência na *Webex* cresceu 22 vezes! (Videoconferência gratuita: o Coronavírus promove ofertas especiais da *WebEx*, Google e outras, 2020). Em tais condições, a confiabilidade das telecomunicações aumenta significativamente.

A cultura corporativa não será a mesma depois do coronavírus. Algumas empresas permanecerão distantes após a epidemia global. Em primeiro lugar, os próprios funcionários, tendo sentido os benefícios do teletrabalho, não quererão voltar aos gabinetes. Em segundo lugar, os proprietários de empresas, tendo medido o KPI dos funcionários e a poupança em instalações e serviços de aluguer, podem deixar apenas os funcionários mais necessários no local.

Medidas de cibercrime e cibersegurança

Se o cibercrime no século passado eram eventos relativamente raros e investigados dentro dos estados individuais, no início do século XXI, eles tornaram-se um dos problemas mais prementes que confrontam a comunidade internacional e começaram a procurar ativamente mecanismos de combate a este fenómeno (Eoghan Casey, 2011, Marie-Helen Maras, 2016), em particular:

- Em 2001, a Convenção sobre Crime Cibernético foi adotada em Budapeste. Este documento estabelece uma lista de crimes cibernéticos e as disposições processuais necessárias para combater o crime cibernético, incluindo a recolha e o partilha de evidências eletrónicas (Convenção sobre Crime Cibernético 2001);
- Em 2002, foi realizado em Londres o Primeiro Congresso Estratégico Internacional sobre Crime Cibernético "Congresso sobre Crime Eletrónico 2002", dedicado aos problemas do combate aos crimes eletrónicos. No congresso, os representantes dos órgãos de aplicação da lei de diferentes países e da indústria de TI discutiram questões de efetiva contração ao crime cibernético (Gutsalyuk M. V. Combate a Crimes Cibernéticos, 2002);
- Em 2004, em conformidade com o Regulamento (UE) n.º 460/2004, foi criada a Agência Europeia para a Segurança das Redes e Informação (ENISA), cuja principal tarefa era melhorar a segurança das redes e da informação na União Europeia (Regulamento (EC) No 460/2004);
- Em 2007, a União Internacional de Telecomunicações (UIT) desenvolveu o Programa Global de Cibersegurança (GCA) como uma estrutura para a cooperação internacional que visa aumentar a confiança e a segurança na sociedade de informação (Agenda Global de Cibersegurança, 2007);
- Em 2010, na ONU, um grupo de especialistas foi criado para realizar pesquisas sobre crimes cibernéticos. O grupo preparou um estudo abrangente sobre o cibercrime (Projeto de Estudo Abrangente sobre Cibercrime, 2013);
- Em 2011, a Estratégia Internacional para o Ciberespaço foi desenvolvida nos EUA. (Estratégia Internacional para o Ciberespaço, 2011);

- Em 2013, foi adotada a Diretiva da UE sobre ciberataques em sistemas de informação (Diretiva 2013/40 / UE);
- Em 2013, em conformidade com o Regulamento (UE) n.º 526/2013, foi criada a Agência da União Europeia para a segurança das redes e da informação e o Regulamento (UE) n.º 460/2004 foi revogado (Regulamento (UE) No 526/2013);
- Em 2013, a Europol criou o Centro Europeu de Cibercriminalidade (EC3) em 2013 para reforçar a resposta da lei ao crime cibernético na UE e, assim, ajudar a proteger os cidadãos, as empresas e os governos europeus da criminalidade online (Centro Europeu do Cibercrime, 2013);
- Em 2014, o Instituto Nacional de Padrões e Tecnologia desenvolveu um Quadro de Infraestrutura Crítica para Instalações de Infraestrutura Crítica para detetar, prevenir e responder a ataques cibernéticos (Quadro para melhorar a segurança cibernética da infraestrutura crítica, 2014). Em abril de 2018, uma nova versão 1.1 deste documento foi lançada;
- Em 2016, foi adotada a Diretiva da UE 2016/1148, relativa a medidas para garantir um elevado nível global de segurança das redes e dos sistemas de informação em toda a União. (Diretiva (UE) 2016/1148, 2016);
- Em 2017, o presidente da Comissão Europeia Jean-Claude Juncker anunciou um pacote de Segurança Cibernética que estabelece medidas para responder ao cenário de mudanças nas ameaças cibernéticas (Pacote de Segurança Cibernética, 2017);
- Em 2018, o Regulamento Geral de Proteção de Dados (RGPD), a diretiva da União Europeia sobre o uso de dados pessoais, entrou em vigor (Regulamento Geral de Proteção de Dados, 2018);
- Em 2019, a Europol anunciou a adoção de um novo protocolo sobre como as autoridades policiais da União Europeia e além responderão aos principais ataques cibernéticos transfronteiriços. O novo protocolo, adotado pelo Conselho da UE, faz parte do Plano de Resposta Coordenada da UE a Incidentes e Crises de Segurança Cibernética Transfronteiriça em Larga Escala, e será implementado pelo Centro Europeu de Cibercrime da Europol (EC3) (UE Adota Novo Protocolo de Resposta para Grandes Ataques Cibernéticos, 2019).

Deve-se notar que, nos últimos anos, todos os países desenvolvidos também adotaram legislação nacional relevante sobre o procedimento penal de crimes cibernéticos, desenvolveram estratégias para combatê-los e criaram as unidades de aplicação da lei apropriadas (Gutsalyuk, 2016).

O estado atual das coisas e os mais recentes desafios da segurança cibernética

No entanto, o cibercrime continua a espalhar-se e crescer. De acordo com pesquisa da PWC (*PricewaterhouseCoopers*), o crime cibernético tinha duas vezes mais hipóteses de ser identificado do que qualquer outra fraude como o crime económico mais perturbador e sério que se espera que cause impacto nas organizações nos próximos dois anos (Pesquisa Económica Global sobre Crime e Fraude da PwC, 2018).

Especialistas do Fórum Económico Mundial em Davos, em Janeiro de 2018, publicaram um relatório anual sobre riscos globais no mundo, intitulado "Relatório Global de Riscos 2018" (Relatório Global de Riscos, 2018) Com base nos seus conceitos, os ataques cibernéticos estão em segundo lugar em termos de influência negativa para a comunidade mundial após eventos climáticos extremos (i.g., há um ano, os riscos tecnológicos e o cibercrime ocupavam o terceiro lugar). O relatório afirma que os riscos de segurança cibernética estão a aumentar constantemente. Por exemplo, os ataques cibernéticos às empresas duplicaram nos últimos cinco anos, e os incidentes que antes eram considerados extremos tornaram-se mais comuns hoje, e *hackers* atacam computadores e redes em "velocidade quase constante" - a cada 39 segundos, há um ataque cibernético (Milkovich Devon, 2019).

O Lloyd's de Londres disse num relatório que grandes ataques cibernéticos globais poderiam desencadear uma média de USD 53 biliões em perdas económicas, incluindo as perdas do ataque WannaCry em maio de 2017, que afetou 300.000 computadores em 150 países, totalizando USD 850 milhões e de ataques a outro vírus de computador que se espalhou na Ucrânia em junho de 2017 totalizaram USD 850 milhões (Gutsalyuk, Klymenko, 2017; Ciberataque global pode gerar perdas de USD 53 biliões, 2017).

De acordo com a estatística de incidentes cibernéticos (ENISA) de 2018, a atividade maliciosa e as falhas do sistema são a principal causa de incidentes relatados: as falhas do sistema representam 39% do total de casos (36% em 2017, respetivamente). O *malware* aumentou para 39% (mais do que 7% em 2017) (Relatório Anual Incidentes de Segurança dos Serviços de Confiança, 2018).

Na era moderna da competição estratégica, a espionagem cibernética está a dar um novo salto. A Escola de Código e Cifra do Governo do Reino Unido (GCCS) estima que existem 34 países diferentes que têm equipas sérias de espionagem cibernética bem financiadas. Essas equipas de atores de ameaças baseadas no estado são compostas por programadores, engenheiros e cientistas informáticos que formam grupos de hackers de agências militares e de inteligência. Eles têm um tremendo apoio financeiro e recursos tecnológicos ilimitados que os ajudam a desenvolver as suas técnicas rapidamente (A espionagem cibernética é global - e está a levar a guerra a um novo nível, 2018).

Uma das mais recentes ferramentas tecnológicas para ataques cibernéticos, atualmente em desenvolvimento ativo, é o uso de *Machine Learning* e inteligência artificial – IA. Como se está a tornar mais fácil criar vírus e realizar ataques em larga escala ao longo do tempo, existe hoje em torno do crime cibernético organizado uma subcultura cibernética maciça, e nos próximos anos, o nível de cibercrime e a auto-organização ativa de *hackers* devem aumentar.

Além disso, cada vez mais países estão a implementar forças cibernéticas que podem influenciar a infraestrutura dos "oponentes". Segundo o secretário-geral da ONU, António Guterres, durante um discurso na Universidade de Lisboa em 19 de fevereiro de 2018: "A próxima guerra começará com um ataque cibernético em massa destinado a destruir as capacidades militares e paralisar a infraestrutura básica, como redes elétricas". Guterres pediu a unificação da comunidade mundial, a fim de minimizar a influência das guerras cibernéticas na vida dos civis e sugeriu a criação de uma plataforma nas Nações Unidas com base na qual cientistas, funcionários e outros poderiam desenvolver regras "para garantir uma natureza mais humana" na resolução de qualquer conflito relacionado com as tecnologias da informação (Khalip Andrei, 2018).

Uma das tendências atuais em tecnologia da informação é a introdução de criptomoedas em larga escala na maioria dos países, que se tornam um instrumento completo de pagamento e um ativo de investimento. A capitalização total de mercado das criptomoedas em 2017 ultrapassou USD 500 biliões. No entanto, deve-se notar que o Bitcoin e outras moedas digitais são adaptadas para uso por grupos criminosos organizados, pois são amplamente utilizados na circulação internacional e fornecem o nível necessário de anonimato. Por exemplo, em 2017, durante o sequestro de pessoas em Kiev, Vinnitsa, Odessa (Ucrânia), cibercriminosos exigiram um resgate numa moeda criptográfica no valor de vários milhões de dólares (Dos 507 sequestros em 4 casos, os autores exigiram um resgate em bitcoins, - Polícia Nacional, 2018).

Devido ao alto custo da criptomoeda, ela atrai os intrusos. Em janeiro de 2018, uma das maiores bolsas digitais no Japão, a Coincheck, relatou uma perda de cerca de USD 534 milhões em criptomoeda devido a um ataque de hackers na sua rede. A Bolsa reembolsará 260.000 clientes às suas próprias custas (Coincheck promete reembolso de 46 biliões de ienes após roubo de criptomoeda, 2018).

Também o termo "cryptojacking" se está a tornar comum - o uso secreto de computadores para minerar a moeda criptográfica. A equipa de pesquisa da Palo Alto Networks 42 revelou uma operação em larga escala na mineração Monero, que está em atividade há 4 meses. O número de vítimas afetadas por esta operação é de aproximadamente 15 milhões de pessoas em todo o mundo (Grunzweig Josh, 2018).

Dado o facto de que a extensão do crime cibernético está a aumentar constantemente, a Interpol, em fevereiro de 2017, desenvolveu uma Estratégia Global de Combate ao Crime Cibernético. O documento afirma que as agências de aplicação da lei enfrentam problemas relacionados com a investigação transfronteiriça, a variedade de legislação e oportunidades tecnológicas em todo o mundo. O programa de combate ao crime cibernético é coordenado pela Interpol através do Complexo Global de Inovação em Singapura, equipado com um laboratório forense digital e um centro de inovação que proporciona à Interpol a capacidade de fornecer uma abordagem consistente e eficaz para combater todas as formas de crime transnacional.

O relatório do Centro Europeu de Cibercrime (EC3) – "Avaliação da Ameaça do Crime Organizado na Internet" – O IOCTA avaliou os principais eventos, mudanças e ameaças no campo do cibercrime em 2019 e chegou ás seguintes conclusões principais:

- O *ransomware* continua a ser a principal ameaça. Os atacantes concentram-se em menos alvos, mas mais lucrativos e maiores danos económicos;
- Os dados continuam a ser um alvo, uma mercadoria e um facilitador importante para o cibercrime;
- Após o aumento do *ransomware* destrutivo, como os ataques do Germanwiper de 2019, há uma crescente preocupação nas organizações com ataques de sabotagem;
- São necessários esforços contínuos para dar ainda mais sinergia ao setor de segurança de redes e informações e as autoridades responsáveis pela aplicação da lei cibernética, afim de melhorar a resiliência e a segurança cibernética em geral;
- A *dark web* continua a ser o principal facilitador on-line para o comércio de uma ampla gama de produtos e serviços criminais e uma ameaça prioritária para a aplicação da lei;

- Grupos terroristas costumam adotar novas tecnologias, explorando plataformas emergentes para as suas estratégias de comunicação e distribuição on-line.

O relatório do Centro Europeu de Cibercrime fornece as seguintes recomendações para combater a cibercriminalidade organizada: a) as agências de aplicação da lei devem continuar a focar-se nos atores que desenvolvem e fornecem ferramentas e serviços para ataques cibernéticos; b) a aplicação da lei e o setor privado devem continuar a trabalhar juntos para analisar ameaças e iniciativas como o projeto *"No More Ransom"* para aumentar a consciencialização e fornecer conselhos e ferramentas gratuitas para decifrar dados de ataques cibernéticos; c) os promotores de *ransomware* de hoje contam cada vez mais com a engenharia social. A formação de funcionários de organizações na deteção de tentativas de engenharia social impedirá muitos ciberataques. Hoje, a probabilidade de roubo de dados pessoais aumentou significativamente (Ao invadir o sistema de informações de uma das empresas, os atacantes apreenderam informações pessoais de 147 milhões de pessoas) (Equifax pagará USD 575 milhões em acordo de violação de dados, 2019). Mais de um milhão de impressões digitais e outros dados sensíveis foram expostos on-line por uma empresa de segurança biométrica, dizem os pesquisadores (Baraniuk Chris, 2019).

Ameaças e desafios futuros

Em geral, podemos afirmar que, atualmente, o número de crimes cibernéticos direcionados a plataformas móveis cresce mais dinamicamente, em que o número de deteções de *ransomware* duplicou nos últimos anos. O desenvolvimento dinâmico da Internet das Coisas (IoT) também é considerado perigoso no ambiente especialista, com o uso do qual se projeta um aumento no número de ataques cibernéticos.

Nesse sentido, o Japão aprovou uma alteração da lei que permite que funcionários do governo invadam os dispositivos de Internet das Coisas (IoT) das pessoas. A alteração faz parte de uma pesquisa que investiga o número de dispositivos IoT vulneráveis, realizado pelo Instituto Nacional de Tecnologia da Informação e Comunicações (NTIC) sob a supervisão do Ministério de Assuntos Internos e Comunicações (MIC). O Japão está a levar a cabo esta pesquisa para impedir que os dispositivos sejam aproveitados para uma infraestrutura de ataque cibernético que suporta os Jogos Olímpicos de Tóquio em 2020. Os funcionários da NICT terão permissão para tentar invadir dispositivos IoT usando senhas e dicionários de senha padrão. Utilizadores que mantêm as senhas definidas como padrão pelo fabricante do dispositivo geralmente levam a que os dispositivos sejam comprometidos. A abordagem do Japão é uma maneira sem precedentes, mas proativa, de lidar com o problema de segurança da IoT. Um relatório publicado pelo MIC destacou que dois terços dos ataques cibernéticos em 2016 foram direcionados para dispositivos de IoT (Daws Ryan, 2019).

Entre os fatores que impedem a luta contra o crime organizado no ciberespaço, continuam os seguintes: a) natureza transnacional das infrações, que consiste no facto de que o local de cometimento, o instrumento do crime, as vítimas e o agressor podem estar sob jurisdições territoriais diferentes e há a necessidade de muitos acordos interestaduais formais para investigar esses crimes, o que diminui significativamente a sua condução; b) alto nível de formação técnica dos criminosos; c) problemas de recolha

de evidências eletrónicas (digitais) que podem ser rapidamente alteradas ou mesmo destruídas; d) a dificuldade em identificar os infratores – uma vez que as "assinaturas" individuais dos infratores são niveladas por um instrumento padronizado de comissão – por software e suporte tecnológico; e) falta de prática judicial suficiente em casos criminais sobre crime organizado no campo da tecnologia da informação.

Devido ao facto de que os dados do computador podem ser facilmente alterados ou mesmo destruídos, os artigos 16 a 21 da Convenção sobre Cibercrime de 2001 preveem a aplicação de medidas legislativas e outras para o armazenamento urgente de dados de computadores, tráfego de dados, intercetação e escala de tempo de registo de informações em tempo real a ser implementada por todos os Estados signatários. É aconselhável trocar essas informações através dos pontos 24/7 relevantes criados em todos os países. No entanto, devido a várias circunstâncias, as respostas às solicitações de tais informações podem ser adiadas por um longo período, tornando essas informações desatualizadas e impedindo a investigação de crimes cibernéticos. Portanto, a cooperação internacional nessa área precisa de melhorias.

Para uma investigação adequada dos crimes cibernéticos, é importante organizar uma cooperação estreita das agências policiais com os prestadores de serviços (Provedores de Internet) para a rápida divulgação de dados e para melhorar os procedimentos de assistência jurídica mútua relacionados a dados eletrónicos, afim de obter prontamente evidências eletrónicas. Ao mesmo tempo, as agências de aplicação da lei já tem uma experiência positiva significativa da cooperação intergovernamental no combate ao cibercrime.

Um exemplo impressionante disso foi a operação para eliminar a rede cibernética "Avalanche", que funcionou durante cerca de 7 anos e infetou milhares de computadores diariamente, e as perdas financeiras por ataques somaram mais de 100 milhões de euros. A investigação foi conduzida pelo Ministério Público de Verdun e pela polícia de Lüneburg (Alemanha) em estreita cooperação com o Ministério da Justiça e o FBI, Eurojust, Europol e parceiros globais. 178 pessoas foram presas por agentes da lei com o apoio do Centro Europeu de Cibercrime (EC3) e da *Taskforce* de Ação Conjunta de Cibercrime (J-CAT) bem como a Eurojust e a Federação Bancária Europeia (EBF). No território da Europa, foram identificados 580 assim chamados "*drones*" (pessoas envolvidas na retirada de dinheiro). Um ataque bem-sucedido a esse grupo criminal organizado internacional foi apoiado por 106 bancos e parceiros privados. Mais de 130 TB de dados recolhidos foram analisados na etapa de preparação de uma operação especial pela ciberpolícia. Durante a operação conjunta, realizada em 30 de novembro de 2016 em 30 países, cinco organizadores da rede foram detidos. Três deles são ucranianos; um foi detido na Alemanha, mais dois - no território da Ucrânia. Um dos organizadores do grupo criminoso é acusado de 1152 crimes, que causaram uma perda de 6 milhões de euros (Rede da Avalanche desmantelada em operação cibernética internacional, 2016).

E em fevereiro de 2018, o Departamento de Justiça dos EUA apresentou uma acusação de fraude cibernética sobre cerca de 36 pessoas suspeitas de participar em grupos internacionais da Organização *Infraud*, criada por um cidadão da Ucrânia. Note-se que o grupo roubou mais de 530 milhões de dólares americanos. A organização recebeu e vendeu ilegalmente dados pessoais de utilizadores de rede, participou em invasões de contas bancárias e eletrónicas e também distribuiu software malicioso. De acordo com as autoridades policiais dos EUA, cerca de 11.000 pessoas estavam envolvidas na

Organização *Infraud*, a maioria das quais nunca se encontrou pessoalmente (Trinta e seis acusados indiciados…, 2018).

Com a crescente popularidade da Internet, e considerando que o comércio eletrónico está a tornar-se a parte mais importante da economia com a rotatividade, medida em triliões de dólares americanos (Vendas a retalho no comércio eletrónico em todo o mundo de 2014 a 2021, 2019), o número de crimes cibernéticos aumentará em conformidade. Portanto, é necessário criar e usar meios de análise de informações nacionais e, idealmente, até internacionais. Além disso, os crimes cibernéticos exigem uma análise por um período menor do que dias, semanas ou até meses, que tendem a basear-se na análise de crimes tradicionais. Ao mesmo tempo, deve-se notar que as organizações de direitos humanos argumentam que grandes quantidades de informações acumuladas não permitem impedir sistematicamente o cibercrime, em vez disso, o armazenamento em massa de dados pessoais abre grandes oportunidades para vários tipos de abuso. Diante disso, em maio de 2014, a decisão do Tribunal de Justiça das Comunidades Europeias (TJCE) declarou que a Diretiva Europeia de Conservação de Dados constituía uma violação grave dos direitos de privacidade ao abrigo do direito europeu e era, portanto, inválido (acórdão do Tribunal de Justiça da União Europeia, 2014).

Finalmente, além de combater o cibercrime, um elemento necessário para o funcionamento seguro e eficiente de uma sociedade digital é a identificação confiável dos seus participantes. Como sabemos, todos os criminosos tentam esconder a sua identidade. Portanto, ao contrário do Darknet, cuja principal característica é o anonimato, é preciso criar serviços eletrónicos que funcionem apenas com utilizadores verificados. É provável que assinaturas digitais eletrónicas ou outros mecanismos, como documentos de identificação eletrónica, sejam usados para verificação para garantir que o utilizador do serviço e o recurso da Internet sejam verificados. Isso, por sua vez, reduzirá significativamente o número de fraudes cibernéticas e outras ofensas no ciberespaço.

Conclusões

Na nossa opinião, entre as questões de efetiva contração ao crime cibernético ainda são relevantes hoje, as seguintes:

1. Elaborar regras legais para a realização de pesquisas de evidências eletrónicas, levando em consideração a possibilidade de encontrá-las em diferentes jurisdições (Khakhanovskyi, Hutsaliuk, 2019).
2. Desenvolvimento de *software* e *hardware* especializados para a recolha, armazenamento e análise de evidências eletrónicas, incluindo grandes casos de evidências informáticas.
3. Melhoria da rede de pontos de contacto nacionais para responder ao cibercrime (24/7) e mecanismos existentes de assistência jurídica internacional.
4. Organização de estreita cooperação entre agências de aplicação da lei e fornecedores para obter evidências eletrónicas.
5. Levantamento regular de qualificações de investigadores e outros agentes envolvidos na aplicação da lei, afim de estudar questões atuais das táticas de condução de ações investigativas para obter evidências eletrónicas na investigação de crimes cibernéticos.

6. Para aumentar a eficácia das investigações sobre crimes cibernéticos, unidades estruturais especializadas devem ser estabelecidas nos gabinetes da polícia e do Ministério Público e, possivelmente, em tribunais especializados.
7. Aumentar o nível de segurança cibernética nos setores público e privado, bem como desenvolver novas tecnologias para proteger e identificar utilizadores do ciberespaço. O Centro Global de Cibersegurança, criado em Genebra sob os auspícios do Fórum Económico Mundial, deve ajudar na estreita colaboração de empresas, académicos e funcionários do governo sobre segurança cibernética.

Apenas através da cooperação de todas as partes interessadas, troca de informações e padrões comuns, a comunidade mundial poderá combater com êxito o cibercrime. O cumprimento dessas medidas permitirá obter plenamente as vantagens da sociedade digital.

Referências bibliográficas

'Avalanche' network dismantled in international cyber operation (The Hague, 01 de dezembro 2016). [Consultado em 16 de setembro 2019]. Disponível em: http://www.eurojust.europa.eu/press/PressReleases/Pages/2016/2016-12-01.aspx.

Annual report Trust Services Security Incidents 2018 [Consultado em 8 de setembro 2019]. Disponível em: https://www.enisa.europa.eu/news/enisa-news/annual-report-trust-services-security-incidents-2018.

Baraniuk Chris. Biostar security software 'leaked a million fingerprints' (14 de agosto, 2019) [Consultado em 15 de setembro 2019]. Disponível em: https://www.bbc.com/news/technology-49343774.

Coincheck promises 46bn yen refund after cryptocurrency theft (28 janeiro, 2018) [Consultado em 10 de setembro 2019]. Disponível em: http://www.bbc.com/news/world-asia-42850194.

Comprehensive Draft Study on Cybercrime (Draft – February 2013) [Consultado em 26 de agosto 2019]. Disponível em: https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf.

Convention on Cybercrime 2001 [Consultado em 23 de agosto 2019]. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Cyber Espionage Is Global – and Taking Warfare to a New Level (2018). [Consultado em 9 de setembro 2019]. Disponível em: https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/.

Cyber Security Package (2017) [Consultado em 3 de setembro 2019]. Disponível em: https://www.dccae.gov.ie/en-ie/communications/topics/Internet-Policy/cyber-security/cyber-security-package/Pages/default.aspx.

Daws Ryan. Japan's law now allows it to hack people's IoT devices (29 de janeiro, 2019). [Consultado em 15 de setembro 2019]. Disponível em: https://www.iottechnews.com/news/2019/jan/29/japan-law-hack-iot-devices/.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (2016) [Consultado em 2 de setembro 2019]. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [Consultado em 28 de agosto 2019]. Disponível em: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040.

Eoghan Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press, 2011. P. 840.

Equifax to Pay $575m in Data Breach Settlement (22 de julho, 2019) [Consultado em 12 setembro 2019]. Disponível em: https://www.phishprotection.com/watchdog/.

EU Adopts New Response Protocol for Major Cyberattacks (2019) [Consultado em 5 de setembro 2019]. Disponível em: https://www.securityweek.com/eu-adopts-new-response-protocol-major-cyberattacks.

EU budget: Commission proposes € 9.2 billion investment in first ever digital programme (Bruxelas, 6 de junho 2018). [Consultado em 23 de agosto 2019]. Disponível em: https://europa.eu/rapid/press-release_IP-18-4043_en.htm.

European Cybercrime Centre (2013) [Consultado em 1 de setembro 2019]. Disponível em: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Framework for Improving Critical Infrastructure Cybersecurity (2014) [Consultado em 2 de setembro 2019]. Disponível em: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11.

Free video conferencing: Coronavirus spurs special deals from WebEx, Google, others URL: [Consultado em 30 de março 2020] Disponível em: https://www.zdnet.com/article/video-conferencing-deals-coronavirus-spurs-offers-from-webex-google-and-others/.

General Data Protection Regulation (2018) [Consultado em 3 de setembro 2019]. Disponível em: https://gdpr-info.eu/.

Global cyberattack could spur $53 billion in losses: Lloyd's of London (2017) [Consultado em 8 setembro 2019]. Disponível em: https://www.cnbc.com/2017/07/17/global-cyberattack-could-spur-53-billion-in-losses-lloyds-of-london.html.

Global Cybersecurity Agenda (GCA) (2007) [Consultado em 26 de agosto 2019]. Disponível em: http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

Global Risks Report 2018 [Consultado em 7 de setembro 2019]. Disponível em: https://www.weforum.org/reports/the-global-risks-report-2018.

Grunzweig Josh. Large Scale Monero Cryptocurrency Mining Operation using XMRig (24 janeiro, 2018) [Consultado em 12 de setembro 2019]. Disponível em: https://unit42.paloaltonetworks.com/unit42-large-scale-monero-cryptocurrency-mining-operation-using-xmrig.

Gutsalyuk Mykhaylo, Klymenko Olga. Combate à criminalidade cibernética e garantias de segurança cibernética na Ucrânia // Lusíada. Política Internacional e Segurança, 2017, nº 15. Pp. 51–65. [online] Disponível em: http://revistas.lis.ulusiada.pt/index.php/lpis/article/view/2506/pdf [Consultado em 2 de Março 2018].

Gutsalyuk Mykhaylo. Ukraine's Cybersecurity Strategy and Ways to Implement It // European Cybersecurity Journal. – Volume 2 (2016). The Kosciuszko Institute. Poland. – P. 65–69. [Consultado em 6 de setembro 2019]. Disponível em: https://twitter.com/i/moments/781827366100140032.

Gutsalyuk M. V. Fighting Cybercrimes (2002) [Consultado em 24 de agosto 2019]. Disponível em: http://www.crime-research.org/library/Gutsaluk.html.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004R0460.

International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World (May 2011) [Consultado em 28 agosto 2019]. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Internet live stats (2019) [Consultado em 23 agosto 2019]. Disponível em: http://www.internetlivestats.com.

Internet Organized Crime Threat Assessment (IOCTA) (2019) [Consultado em 11 outubro 2019]. Disponível em: https://www.europol.europa.eu/iocta-report.

Judgment of the Court of Justice of the European Union (Date of decision/judgment: 13/05/2014) / ECLI:EU:C:2014:317. [Consultado em 17 setembro 2019]. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

Khakhanovskyi Valerii, Hutsaliuk Mykhaylo. The Peculiarities of Digital Evidence Use in Criminal Proceedings // Kryminalistychnyi Visnyk, Vol 31, No 1 (2019). pp. 13–19. DOI: https://doi.org/10.37025/1992-4437/2019-31-1-13.

Khalip Andrei. U.N. chief urges global rules for cyber warfare (19 fevereiro, 2018) [Consultado em 8 setembro 2019]. Disponível em: https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4.

Marie-Helen Maras. Cybercriminology. Oxford University Press, 2016. P. 448.

Milkovich Devon. 15 Alarming Cyber Security Facts and Stats (23 setembro, 2019) [Consultado em 25 setembro 2019]. https://www.cybintsolutions.com/cyber-security-facts-stats/.

Of the 507 abductions in 4 cases, the perpetrators demanded a ransom in bitcoins, – National Police (26 janeiro, 2018) [Consultado em 10 setembro 2019]. Disponível em: https://112.ua/obshchestvo/iz-507-pohishheniy-v-4-sluchayah-zloumyshlenniki-trebovali-vykup-v-bitkoinah-nacpoliciya-430498.html.

PwC's Global Economic Crime and Fraud Survey 2018 [Consultado em 6 setembro 2019]. Disponível em: https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html.

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) [Consultado em 25 agosto 2019]. Disponível em:

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (Text with EEA relevance) [Consultado em 1 setembro 2019]. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0526.

Retail e-commerce sales worldwide from 2014 to 2021 (in billion U.S. dollars) / By J. Clement, editado pela última vez em 30 de agosto 2019 [Consultado em 17 setembro 2019]. Disponível em: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/.

Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrimes (Wednesday, February 7, 2018) / Department of Justice / Office of Public Affairs. [Consultado em 16 setembro 2019]. Disponível em: https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible.