КИБЕРСИГУРНОСТТА – МЕЖДУНАРОДНИ И НАЦИОНАЛНИ ИЗМЕРЕНИЯ

д-р Мария Йорданова
Център за изследване на демокрацията

CYBERSECURITY – INTERNATIONAL AND NATIONAL DIMENSIONS

Maria Yordanova, PhD
Center for the Study of Democracy

Abstract: *The report provides an overview of: policies and practical measures for tackling cybercrime and for ensuring cybersecurity within the European Union and the Member States; international instruments and cooperation; private sector initiatives to develop standards for cybersecurity and information sharing on emerging cyber threats and risks; successful public-private partnerships, co-regulations, self-regulations; public perceptions of crime and security in cyber space.*

Key words: *cyber policy, cybercrime, cybersecurity, internet, digital.*

1. Общи бележки

Сигурността е ключова област на международната политика. Дигиталната ера, наред с големите предимства, от които всеки ежедневно се ползва в личния живот, професията, обучението, комуникациите си, включително с институциите, поставя и големи предизвикателства пред сигурността и човешките права. Последиците от тези предизвикателства могат да засегнат не само отделните индивиди, групи хора, нации, държави и по-широки общности, но и света като цяло. В този контекст международната политика за **киберсигурност** се превръща в съществена част от бъдещия глобален ред.

Интернет вече е една от най-важните инфраструктури в света, чиито мащаби и темпове на развитие откриват неограничени перспективи за модернизиране и подобряване на живота. В същото време, интернет все повече е и среда, в която се извършват високотехнологични неправомерни действия и престъпления (напр. злонамерени атаки срещу информационните системи, зловреден софтуер), онлайн тормоз, онлайн сексуална експлоатация на деца, измами с плащания, както и среда, в която джихадисти и терористи набират своите поддръжници и бойци, извършат пропаганда и т.н. Терористичната пропаганда се разпространява от една страна, в рамките на малки мрежи и местни онлайн общности, а от друга – в глобални платформи като Twitter, Facebook и Tumblr, където терористите могат да намерят по-голям брой необразовани и зле информирани хора. Чрез дезинформация и пропаганда терористите обаче успяват да спечелят на своя страна и добре образовани лица от държавите – членки на ЕС, които най-често се чувстват социално и културно изолирани в обществото.

Развитието на новите информационни технологии съществено промени и природата на престъпността – както традиционните престъпления, които се извършват в

киберпространството, така и специфичните компютърни престъпления, не познават граници и разкриват висока обществена опасност. Те сериозно заплашват човешките права, националната и международната сигурност. За голяма част от тези незаконни действия няма адекватна законодателна уредба и в много отношения технологичното развитие продължава да изпреварва еволюцията на нормативната уредба на международно и национално равнище.

Информационно-технологичните достижения дават огромен простор за упражняване на човешките права и свободи, но същевременно те са вече по-уязвими от всякога. В новата комуникационна среда на изпитание са поставени неприкосновеността на личния живот, сигурността и защитата на личните данни. Човешките права се нарушават не само от киберпрестъпността и киберзаплахите. Нарастват рисковете за ограничения на човешките права от правителствата и политиците, които под претекст за гарантиране на сигурност или мнима защита на правата могат да налагат цензура, забрани, да упражняват нелегитимен натиск върху гражданите и частния сектор. Забраната на турското правителство през март 2014 г. за достъп до Twitter, използван наред с Facebook и други социални медии от протестиращите по време на антиправителствените демонстрации в Турция през 2013 г., е ярък пример за това. Официално забраната е наложена на основание, че Twitter не премахва съдържание, което нарушавало правото на личен живот чрез популяризиране на изтекли записи на телефонни разговори, претендиращи да докажат широко разпространената корупция сред правителствени служители и хора, близки до тогавашния премиер и настоящ президент Ердоган (който твърди, че противниците му са изфабрикували записите), включително и сина му.[1]

2. Международни политики и инициативи

Най-влиятелните международни организации чрез различни инициативи и политики търсят отговор на нарастващите глобални кибер заплахи.

Киберсигурността е важен приоритет за **Организацията на обединените нации**[2] и на редица свързани с нея или под нейната егида организации като

[1] Съдът в Анкара уважи жалбата на Колегията на турските адвокати и Съюза на журналистите и обяви забраната за нарушаваща свободата на информация и комуникации като задължи телекомуникационните компании да възстановят достъпа до услугата. След решение на Конституционния съд на Турция, че правителствената забрана нарушава законите, регулиращи свободата на изразяване, достъпът до Twitter е възстановен през април 2014 г., но блокът на YouTube се запазва и след това. За повече информация: The New York Times, Turkish Court Overturns the Government’s Ban on Twitter, by Sebnem Arsu, 26 March 2014, available at: http://www.nytimes.com/2014/03/27/world/middleeast/turkey-twitter.html?_r=1; Turkey’s constitutional court rules against YouTube block, in: ComputerWeekly.com, 30 May 2014, available at: http://www.computerweekly.com/news/2240221574/Turkeys-constitutional-court-rules-against-YouTube-block

[2] Общото събрание на ООН от средата на 80-те години досега е одобрило редица резолюции и други инструменти, насочени срещу заплахите в областта на информационната сигурност, както и възможните мерки за ограничаване на заплахите, за подобряване на информираността относно сигурността в кибернетичното пространство, както на международно, така и на национално ниво. В частност Резолюция 64/211, приета през декември 2009 г. и насочена към създаването на глобална култура на киберсигурността, прави преглед на националните усилия за защита на критичните информационни инфраструктури. За повече информация: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211

Международната агенция за атомна енергия (МААЕ), Службата на ООН по наркотиците и престъпността (UNODC)[3], Международния съюз по далекосъобщения (ITU), Междурегионалния изследователски институт по престъпността и правосъдието на ООН (UNICRI) и др. Инициативите на ООН и редица нейни агенции (често в сътрудничество с партньори като Интерпол, Съвета на Европа и ОИСР) допринасят за формулиране на нови политики за киберсигурност. Конкретни действия (като ITU's Global Cybersecurity Agenda) са насочени към укрепване на глобалната общественото доверие и сигурност в използването на ИКТ чрез изграждане на синергии и ангажиране на всички заинтересовани страни.

Въпреки усилията на ООН досега и въпреки предимствата й като глобална многофункционална международна организация в координирането на международните позиции и действията на държавите членки, все още не съществува глобално споразумение и единна политика по отношение на киберсигурността.

Организацията за икономическо сътрудничество и развитие още през 80-те години инициира развитие на международни и национални политики срещу компютърните престъпления.[4] Усилията на организацията се съсредоточават и върху необходимостта от повече знания и разбиране на въпросите на сигурността и развитието на култура на сигурност. Съвременният фокус на инициативите й са киберсигурността и развитието на глобални координирани политики за създаване на доверие. [5]

Съветът на Европа играе много важна роля в развитието на наднационална политика срещу заплахата от киберпрестъпността чрез Конвенцията за компютърните престъпления (Будапещенска конвенция, в сила от 2004 г.) и Допълнителния протокол на ксенофобията и расизма[6]. Конвенцията се опитва не само да дефинира компютърните престъпления, но и да подпомогне разработването на политики за предотвратяването им, както и създаването на основа за международно сътрудничество в разследването и преследването на престъпленията в киберпространството, за създаване на разпоредби за взаимна помощ и процедури за екстрадиране. Конвенцията и свързаните с нея инструменти са повратна точка в международните усилия срещу киберпрестъпността и важна стъпка към по-широк консенсус между правителствата. Въпреки ограниченото прилагане на разпоредбите на Конвенцията, както и липсата на механизъм, който да гарантира, че страните изпълняват своите задължения по конвенцията, тя има потенциал за развитие и разширяване.

---

[3] За повече информация виж: UNODC: Role in global response to Cybercrime, September 2011, available at: http://www.itu.int/ITUD/asp/CMS/Events/2011/CyberCrime/S9_UNODC.pdf, also: "UNODC & the Global Response to Cybercrime" (ppt), достъпен на: https://www.unodc.org/documents/southeastasiaandpacific//2011/09/cybercrimeworkshop/ppt/Cybercrime_Asia2_Sept_2011.pdf; Cybercrime: The Global Challenge, 2011: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf;Comprehensive Study on Cybercrime. New York: United Nations, достъпен на: http://www.unodc.org/documents/commissions/CCPCJ_session22/13-80699_Ebook_2013_study_CRP5.pdf

[4] Organisation for Economic Co-operation and Development (1986): Computer-Related Crime: Analysis of Legal Policy. Paris: Organisation for Economic Co-operation and Development, достъпен на: http://www.oecd.org/

[5] Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002, достъпни на:
http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm

[6] Convention on Cybercrime. In: European Treaty Series No.: 185. Budapest: Council of Europe, достъпна на: http://conventions.coe.int/Treaty/en/Treaties/Html/185.

Сред основните дефицити в международен план са липсата на унифицирана международна политика за киберсигурност и ограниченото практическо прилагане на създадените инструменти, включително поради различията в правните системи и различните приоритети на отделните държави.

3. *Ролята на Европейския съюз*

Европейският съюз (ЕС), утвърдил се като важен фактор в международните отношения в периода след студената война, успешно разширява влиянието си през последните две десетилетия. Проблемите на киберсигурността все повече са в центъра на вниманието на ЕС. Наред с приемането на правни инструменти, регулиращи някои специфични компютърни престъпления (атаки срещу информационни системи, сексуални злоупотреби и детска порнография), държавите членки и Европейската комисия (ЕК) признават като приоритет необходимостта от развитието на специална политика на Съюза за подобряване на киберсигурността и предприемат стъпки в тази посока.

3.1. Инициативи за развитие на обща политика за подобряване на киберсигурността

Европейската комисия (ЕК) през 2001 г. със *Съобщение за създаване на безопасно информационно общество чрез подобряване на инфраструктурите за сигурността на информацията и за противодействие на компютърните престъпления* предлага редица материално- и процесуалноправни норми за борба с престъпността в национален и наднационален мащаб. То е последвано от поредица рамкови решения, сред които Рамково решение 2005/222/ПВР за атаките срещу информационните системи.

През 2007 г. ЕК започва обща политическа инициатива за подобряване на координацията в борбата срещу компютърната престъпност на европейско и международно равнище чрез *Съобщение до Европейския Парламент, Съвета и Комитета на регионите: към обща политика за борбата срещу компютърната престъпност*. Споделя се разбирането за необходимостта от незабавно предприемане на действия срещу всички форми на тази нова престъпност, която засяга съществено критичната инфраструктура, обществото, бизнеса и гражданите, като приеме политическа рамки на Съюза, съгласувана със съответните европейски и международни организации. Фокусът на инициативата е укрепването на наказателното право и капацитета на правоприлагащите органи в киберсредата, да се подобри координацията и сътрудничеството между специализираните звена, съответните власти и експерти, политическото и правното партньорство с трети държави, да се засили диалогът с частния сектор.

През 2013 г. е обявен първият задълбочен цялостен политически документ *Стратегия за киберсигуронст на ЕС: открито, безопасно и сигурно киберпространство* (със съвместно съобщение до Европейския Парламент, Съвета на Европейския икономически и социален съвет и Комитета на регионите, ЕК и Върховния представител на ЕС по външните работи и политиката по сигурността)[7]. Стратегията

[7] European Commission, High Representative of the Union (2013): Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, (JOIN (07 February 2013) 01 final), Brussels: European Commission, High Representative of the European Union for foreign affairs and security policy, достъпна на: http://new.eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:52013JC0001&rid=8

обхваща сферите на вътрешния пазар, правосъдието и вътрешните работи, както и външнополитическите аспекти на киберпространството. Към нея е приложено предложение за законодателни мерки за засилване на сигурността на информационните системи в ЕС с цел да се поощри икономическия растеж чрез доверието в онлайн продажбите и използването на интернет. Стратегията адресира всички релевантни действащи лица – публичната власт, частния сектор и отделните граждани, и определя ръководните принципи в политиката по киберсигурност в ЕС и в международен план:

- прилагане на ценностите на ЕС, отнасящи се до физическия свят, и в дигиталния свят (прилагане на същите закони и норми);
- защита на основните права и свободи, защита на личните данни и пространство като основа на политиката на киберсигурност;
- безопасен достъп на всички до интернет и безпрепятствен обмен на ин-формация;
- демократично и ефективно управление с участие на всички заинтересовани страни;
- споделена отговорност за гарантиране на киберсигурност.

Стратегията поставя като задача държавите членки да вземат мерки срещу предизвикателствата в киберпространството и определя 5 стратегически приоритета: постигане на киберустойчивост, драстично намаляване на компютърните престъпления, развитие на обща политика за киберсигурност и защита, развитие на индустриални и технологични ресурси за киберсигурност, създаване на международна политика на ЕС относно киберпространството, основана на европейските ценности.

Във връзка с борбата срещу киберпрестъпността се поставят конкретни стратегически цели: силно и ефективно законодателство на равнище ЕС и държавите членки, оперативен капацитет на всички национални правоприлагащи органи и по-добра координация на равнище на общността. За тази цел се обръща внимание на необходимостта: да се осигури транспониране и прилагане на всички директиви по темата, включително държавите членки, които не са ратифицирали Конвенцията на Съвета на Европа по компютърните престъпления, да го направят в най-кратък срок и да я приложат; да се засили способността за разследване и противодействие на киберпрестъпността, засилване на връзките между научните изследвания, правоприлагащите органи и частния сектор.

3.2. Практически резултати в политическото, институционалното и технологичното развитие в ЕС и държавите членки

Внимание заслужава създаването на институционални механизми за прилагане на стратегията и политиките за киберсигурост. **Европейската мрежа и агенция за информационна сигурност (ENISA)** е създадена през 2004 г., а през 2010 г. е приета нова регулация за нейното модернизиране и нов мандат. Главната й цел е да стимулира сътрудничеството между публичния и частния сектор и да оказва съдействие на ЕК и на държавите членки, да координира превенцията, разкриването и разследването на компютърните престъпления в държавите членки.[8] Агенцията играе важна роля и в контактите с Европол, с частния сектор и в сътрудничеството с трети държави.

[8] За повече информация: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss

Европейският център за компютърни престъпления (EC3) е създаден през 2012 г. за борба с престъпността в дигиталната ера с цел да бъде контактна точка на ЕС в рамките на Европол в борбата срещу киберпрестъпността и да подпомага ЕС и държавите членки в разследванията, да сътрудничи с международни партньори[9]. Официално започва работа на 1 януари 2013 г. с мандат да предоставя оперативна подкрепа на правоохранителните органи от държавите – членки на ЕС и извън ЕС за справяне с компютърните престъпления в различни сфери, като например престъпленията в кибернетичното пространство, извършени от организирани престъпни групи (особено тези, генериращи големи престъпни печалби като онлайн измами); киберпрестъпленията, които причиняват сериозна вреда на техните жертви, като онлайн сексуална експлоатация на деца; киберпрестъпленията (включително кибератаки), засягащи критичната инфраструктура и информационни системи в рамките на Съюза и т.н.

Мобилната индустрия, един от най-бързо развиващите се сектори на интернет, е доминирана от европейски технологии. Въпреки масираното изтичане на мозъци от Европа към САЩ, Европа има водеща роля във въвеждането на глобални стандарти, а почти 50% от трафика на мобилния интернет преминава през европейската инфраструктура. Наред с това, инициативите на ЕС и развиващите са публично-частни партньорства целят да предпазят децата и младите хора от киберзаплахите. Примери за това са: създаването на „горещи линии” за получаване на сигнали за незаконно и вредно съдържание и други прояви на престъпно поведение в киберсферата; европейската рамка за безопасно използване на мобилни услуги от тийнейджъри и деца, приета от европейската мобилна индустрия и включена в националните кодекси за поведение на мобилните оператори в почти всички държави членки и т.н.

На национално ниво, отговорът на държавите – членки на ЕС на киберзаплахи варира, но фокусът е върху предприемане на мерки за засилване на киберсигурността, за противодействие и превенция на киберпрестъпността. Различни национални инициативи са насочени към подобряване на координацията и увеличаване на експертните познания в областта на киберпрестъпността. Националните правителства сътрудничат с частните предприятия и държавния сектор, включително в сферата на образованието, за да се насърчи увеличаването на сигурността на киберпространството. Други национални дейности са насочени към повишаване на осведомеността на потребителите на интернет за различните заплахи. Например, полицейска програма за превенция на престъпността в Германия образова гражданите относно видовете кибератаки и посегателства (фишинг, вируси, троянски коне, мрежи и кибертормоз) и възможностите те да бъдат предотвратени; Финландският иновационен фонд (Sitra), създаден в рамките на финландския парламент, цели създаването на основни международни правила за справяне с кибератаки, и за подобряване на разбирането на хората за сигурността на киберпространството.

В последно време все повече държави членки разработват и приемат специфични национални политики и стратегически документи в тази сфера при засилен ангажимент на националните правителства за осъществяване на планираните мерки. Стратегията за киберсигурност на Финландия предвижда създаването на модел за сътрудничество между национални и международни органи (например Европол и Интерпол) и други участници – стопански организации, полиция, финландските сили за отбрана и съответните неправителствени участници, с цел повишаване на нацио-

[9] За повече информация: https://www.europol.europa.eu/ec3

налната сигурност в киберпространство и киберотбраната. Стратегията на Германия подчертава важността на сътрудничеството и координацията на органите, които се занимават с въпросите на киберпрестъпленията. Стратегията на Великобритания определя, че начинът за справяне с киберзаплахи трябва да балансира сигурността със спазването на неприкосновеността на личния живот и основните права, както и да гарантира, че киберпространството е отворено за иновации и за свободното движение на идеи, информация и изразяване. Испанската стратегията идентифицира рисковете и заплахите за сигурността на киберпространството и предвижда създаването на Специализираната комисия по киберсигурност с мандат да координира националната политика за киберсигурност и да подкрепя министър-председателя и Съвета за национална сигурност и Специализирания ситуационен комитет при управлението на кризисни ситуации в тази област.

България е една от последните държави членки, която приема национална стратегия („Кибер устойчива България 2020“) едва през юли 2016 г. Предвиденият в стратегията модел за функциониране на национална система за киберсигурност трябва да осигурява непрекъснат мониторинг на националната киберкартина и киберсъстоянието във всички сегменти на управление и функциониране на държавата, икономиката, и обществото. Предвижда се създаването на Съвет по киберустойчивост към Министерския съвет с направляващи и стратегически функции. [10]

Националните политики по киберсигурност обикновено се ръководят и координират от правителствата и съответните министерства с участието на правоприлагащите органи. В някои държави членки съществуват и местни политически инициативи (Германия, Испания). Два важни общодържавни механизъма за разследване са създадени в рамките на двете полицейски сили на Испания – националната полиция и на гражданската гвардия. Във Великобритания централно полицейско звено за е-престъпления, финансирано съвместно от Министерството на вътрешните работи и Лондонската полиция, разследва най-сериозните прояви на киберпрестъпността и си сътрудничи с международните правоприлагащи органи.

Всички държави членки полагат усилия за укрепване на институционалния си капацитет за борба с киберпрестъпността и разработване на необходимата инфраструктура чрез създаване на специални структури, като новосъздадените звено за Националната киберпрестъпност в Обединеното кралство, Национален Център за киберотговор в Германия и т.н.

Има много други правителствени инициативи за повишаване на киберсигурността, които са насочени общо към индустрията, банките, доставчиците на интернет услуги и потребителите (в Обединеното кралство и Германия), както и политически

[10] Правомощията на Съвета по киберустойчивост включват: да следи тенденциите и развитието на кибер заплахите, рисковете, методите за противодействие и необходимите способности, приоритетите за изграждането и развитието на човешки, технологичен, инфраструктурен, финансов, организационен и доктринален компоненти и при необходимост ще внася предложения пред Съвета по сигурност към Министерския съвет за решения; да подготвя периодичен доклад за Съвета по сигурността и за Министерския съвет за състоянието на сигурността в киберпространството, развитието на рисковете и обобщената оценка на постигнатото ниво на зрялост и киберустойчивост. изработване и обосноваване на позицията на България пред международни институции и организации по въпросите на киберсигурността; да наблюдава изпълнението на проектите от Плана за действие и пътната карта по стратегията. За повече информация: https://www.actualno.com/politics/prieta-e-nacionalna-strategija-za-kibersigurnost-news_550488.html; http://cyberbg.eu/

инициативи (в България и Испания), свързани с конкретни социални сектори (образование) или групи (деца, потребители).

Някои страни разработват и изпълняват стратегии за междусекторно сътрудничество и програми извън системата на наказателното правораздаване, стратегии за сътрудничество между публичните и частните участници (Финландия), както и партньорства ad hoc, с цел по-адекватна превенция и противодействие на киберпрестъпността. Наред с националното сътрудничество между правителствата и органите на реда, с участието на широк спектър от организации, образователни институции и физически лица, в процес на засилване е регионалното и международното сътрудничество.

Националните усилия са все повече се ориентират към това да се дава координиран съвместен трансграничен отговор на нарастващите киберзаплахи. В Германия Министерството на външните работи разглежда киберполитиката като оказваща влияние върху почти всички области на външната политика и във връзка с това през 2013 г. е назначен комисар по международна киберполитика.

В обобщение, състоянието на националните и международните усилия срещу киберпрестъпността разкрива необходимостта от по-добра координация и ангажимент за приемане на подходящи глобални решения, регулации и проактивно действие на много нива.

Частният сектор има активна роля за засилване на сигурността на киберпространството. Бизнес и неправителствени организации, макар и доброволно, са движещата сила за иницииране на доброволни (незаконодателни) мерки за саморегулиране на интернет чрез кодекси за поведение и етични кодекси. Те често включват механизми за санкциониране на неподходящо поведение онлайн чрез оплаквания от други потребители на интернет (например, Дружеството на електронни съобщения в България) или извънсъдебни механизми за решаване на спорове (като Confianza онлайн в Испания). Частният сектор също осигурява финансови ресурси и техническа експертиза за подкрепа на правоприлагащите органи и националните правителства за намаляване на вредите от киберпрестъпността, например, подпомагане на правителствата да приложат програми, които са по-устойчиви на кибератака.

Съвместното **публично-частно регулиране** се насърчава от Европейския съюз и чрез местни политики. Има различни примери за това. В Обединеното кралство схема за професионално сертифициране (2012 г.), създадена от частния сектор, установява стандарти за качество както на информацията, предоставена чрез интернет, така и за професионалистите, работещи в публични и частни мрежи; и ръководни принципи за киберсигурност (2013 г.), развити съвместно от правителството и интернет индустрията с цел да информира, образова и защитава клиентите на доставчиците на интернет услуги. Има и образувания, които насърчават сътрудничеството между публичния и частния сектор за борба с незаконната дейност в интернет, като например Виртуален общинско-полицейски екип във Финландия, Съвет за национална киберсигурност в Германия, и Обществен съвет за безопасен интернет в България.

Друга област на **публично-частно партньорство** в рамките на ЕС включва инициативи за защита на децата и младите хора от киберзаплахи. Те включват образователни и разяснителни дейности, кампании и събития, насочени към децата, учителите и родителите, както и общи потребители на интернет и мобилни услуги за насърчаване на безопасното използване на интернет и повишаване доверието на потребителите в киберсигурността. Така например, уеб сайтове (част от международната

мрежа, ръководена от INHOPE) предлагат инструкции и техники за саморегулиране и програми за защита. Някои уеб сайтове поддържат горещи линии за получаване на онлайн съобщения за незаконно и вредно съдържание и други видове киберпрестъпно поведение. Освен това, Европейската мобилната индустрия е приела *Европейската рамка за безопасно използване на мобилни телефони от юноши и деца* и това е включено в националните кодекси на поведение в почти всяка държава членка.

3.3. Дефицити и слабости

Въпреки скицираните инициативи и постижения (на равнище на общността и на частния сектор) Европа изостава в развитието на глобална политика за киберсигурност и адекватна защита на човешките права в дигиталната ера. В обобщен вид слабите страни се свеждат до следното:

- Много от усилията засега остават фрагментарни.
- Политическите и законодателните мерки за засилване на киберсигурността и противодействие на нарушенията на човешките права в киберпространството имат ограничен ефект.
- Няма консенсус кои кибернарушения да се криминализират, нито общоприета дефиниция за класифициране на компютърните престъпления.
- Поради липсата на сравнителни данни за незаконните действия в киберпространството няма яснота и реална оценка за разпространението на компютърните престъпления в ЕС.
- **Обществеото доверие,** както в киберсигурността, така и в способността на институциите ефективно да контролират киберпространството в интерес на сигурността и при спазване на човешките права, е ниско. Въпреки всички специфики на отделните държави, включително и различни нива на използване на интернет и на използване на интернет за услуги (като онлайн банкиране или купуват неща онлайн), данните на специалните изследвания на Евробарометър за киберсигурността, публикувани от Европейската комисия през 2012, 2013 и 2015 г., удостоверяват висока степен на загриженост на потребителите на интернет и опасения да не станат жертва на киберпрестъпления. Проучването показва, че всяка поредна година гражданите на ЕС са по-загрижени за проблемите на киберсигурността, отколкото са били през предходната година. [1,2,3] Други изследвания показват, че въпреки широко разпространените опасения от виктимизация, малка част от жертвите на киберпрестъпления съобщават за това на полицията. Същевременно, резултатите за нивото на доверие на респондентите в интернет сигурността варира според страната. Например, анкетираните във Финландия показват значително по-голяма увереност в използването на услуги, изискващи онлайн плащане от анкетираните в Италия или България, където съотношението на тези, изразяващи доверие е, съответно една пета (Италия) и една десета (България) от това, отчетено във Финландия. Отчасти това може да се обясни с по-широкото използване на този вид услуга от финландските анкетирани, което е три пъти по-високо, отколкото в Италия, и 10 пъти по-високо, отколкото в България. [11]

[11] За изследванията, проведени в периода 2014 - 2015 г. в група държави членки, виж Policy Brief on cybercrime, достъпен на: http://fiduciaproject.eu/fiducia_policy_briefs

• Макар че ЕС взема предвид съществуващите международни инструменти и е в контакт с много международни структури (такива като Съвета на Европа, ООН, Организация за икономическо сътрудничество и развитие, Организацията за сигурност и сътрудничество в Европа, НАТО и др.), съвместното национално координиране на политиките и международното сътрудничество е недостатъчно.

Така, въпреки постигнатия напредък като водеща сила в глобалната система, Европа все повече губи позициите си поради невъзможност да се справи с настоящите кризи (в частност, бежанската и мигрантската, терористични атаки) и други съвременни предизвикателства с глобални, регионални и национални измерения. В тези условия е все по-трудно ЕС да упражнява влияние и да влияе конструктивно върху световния ред. Светът се променя и с това и мястото на Европа в него. Това се проявява и по отношение на киберполитиката.

На тези тенденции все по-голямо внимание обръщат изследователи и политици. Някои автори изказват предположения, че най-правдоподобната бъдеща роля на ЕС в новия баланс на глобалната система ще е на „цивилна сила“ с регионална насоченост.[4] Други акцентират върху промяната на международния ред, намаляването на конкурентоспособността на Европа, както и необходимостта от вътрешни компромиси по време на последните няколко години, които са започнали да разколебават вярата в бъдещите способности на Съюза активно да влияе върху по-широкото европейско пространство, и в неговото адаптиране към променящата се глобална среда.[5]

В речта си *Европейският съюз в новия световен ред* пред училището по мениджмънт на Йелския университет през 2014 г. бившият председател на Европейската комисия Барозу заявява, че „основният въпрос на нашето време е дали ще успеем да се адаптираме към променящата, сложна и предизвикателна глобална среда и как“ и изразява убеждението си, че промяната, в краткосрочен план, изисква лидерство, както и по-силна легитимност.[12]

Естонският президент Томас Хендрик Илвес в реч пред Европейския парламент на 2 февруари 2016 г. посочва като важно предизвикателство пред Европа дигиталната революция, както и необходимостта Европа да бъде в крак с новите технологии, за да не изостава от САЩ, Китай и Индия. Като отчита дълбоката промяна, настъпила в последните 10-15 години, той предлага наред със свободното движение на хора, стоки, капитали и услуги, да се въведе нова, пета свобода – **свободното движение на данни** (включваща придружаващите я права и задължения – от една страна, правото на всеки човек да контролира използването на неговите лични данни и предаването им на трети лица, а от друга – създаване на „икономика на данни”, основана на потенциала на големите набори от данни при запазване на информационната неприкосновеност на личния живот). Във връзка с това той подчертава, че посрещането на предизвикателството на дигиталната революция изисква „изобретателността на предприемачите в Европа, бизнеса, гражданското общество и всички нива на управление.”[13]

[12] http://europa.eu/rapid/press-release_SPEECH-14-612_en.htm

[13] Address of President Toomas Hendrik Ilves at the European Parliament, February 2, 2016, available at: https://president.ee/en/official-duties/speeches/11972-address-of-president-toomas-hendrik-ilves-at-the-european-parliament-february-2-2016/index.html

4. Заключение

Постигнатото ниво на консенсус за формирането на обща политика на киберсигурността (между правителствата, международните и наднационалните организации, бизнеса и третия сектор) остава ниско. Все още липсва споразумение по-широк кръг от въпроси на киберсигурността и киберпрестъпността, необходимо за да се гарантира ефективното правоприлагане. В отсъствието на ясно изразен диалог и съвместен подход към информационната и киберсигурността от глобална гледна точка, възникват отношения и се сключват споразумения на двустранно равнище (споразумението за „информационна сигурност“, сключено между Китай и Русия през 2015 г., споразумението между САЩ и Русия от 2013 г. за изграждане на доверие в киберсигурността), които могат да нарушат необходимото равновесие в международната политика по отношение на киберпространството.

Бързото развитие на Интернет и новите технологии и тяхното въздействие на политиката предизвиква широк спектър от национални, международни и обществени организации и частни лица да се включат във формирането на политики и решения. Техните усилия трябва да бъдат интегрирани в по-единни действия. Приетите конвенции и други инструменти на ЕС и на международно равнище осигуряват стабилна основа, върху която може да се основава на международни политики и сътрудничество. Те трябва да се разширят (нормативно и регионално) и да се актуализират редовно с цел по-ефективно противодействие на киберпредизвикателствата на различни нива. Паралелно с това са необходими по-силни европейски и международни публично-частни партньорства, саморегулации на частния сектор и инициативи на гражданското общество, които да допринесат за превенцията и противодействието на киберзаплахите, както и за развитието и прилагането на глобална политика за киберсигурност.

В бъдеще области като икономика, политика, комуникации, финансова система и т.н., ще бъдат още по-зависими от функционирането на мрежата. Изследванията предвиждат ръст на киберзаплахи, като например увеличаване използването на услуги, включващи извършването на компютърни престъпления, разработване на все по-сложен зловреден софтуер, пренасочване на зловредния софтуер към мобилни устройства, повишена хакерство при облачните услуги за целите на шпионаж и т.н. Киберпредизвикателствата ще продължат да пресичат националните граници и юрисдикции, поради което сигурността на киберпространството неизбежно се превръща в проблем от световно значение, справянето с който изисква глобален, изпреварващ и динамичен подход.

Цитирана литература

1. European Commission (2012): Special Eurobarometer 390 on Cyber Security, Report, July 2012, available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf
2. European Commission (2013): Special Eurobarometer 404 on Cyber Security, Report, November 2013, available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf
3. European Commission (2015): Special Eurobarometer 423 on Cyber Security, Report, February 2015, available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

4. Maull, Hanns W., Europe and the New Balance of Global Order, in: International Affairs (Royal Institute of International Affairs 1944) Vol. 81, No. 4, Britain and Europe: Continuity and Change (Jul., 2005), pp. 775-799, available at: http://www.jstor.org/stable/3569674?seq=1#page_scan_tab_contents
5. Balázs, Péter, Europe's position in the new world order, 2013, available at: http://www.ceupress.com/books/html/Europe's%20_Position_in_the_New_World_Order.htm

Използвана литература

1. Thomas, Rachel Nyswander (2012, updated 2013): Securing Cyberspace through Public-Private Partnership: A Comparative Analysis of Partnership Models, available at: http://csis.org/files/publication/130819_tech_summary.pdf
2. UK Government, Department for Business, Innovation and Skills (2013): Guiding Principles on Cyber Security (Guidance for Internet Service Providers), available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265328/bis-13-1327-guiding-principles-for-cyber-security-isps-and-hmg-FINAL.pdf
3. Schneider, Christoph/Katzer, Catarina/Leest, Uwe (2013): Cyberlife – Spannungsfeld zwischen Faszination und Gefahr: Cyberlife – Between the priorities of Fascination and Danger, available at: http://www.buendnis-gegen cybermobbing.de/Studie/cybermobbingstudien.pdf
4. KPMG (2014): Cybercrime Survey Report, available at: https://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG_Cyber_Crime_survey_report_2014.pdf
5. Observatorio Nacional de las Telecomunicaciones y de la Seguridad de la Información,
6. (2014): Ciberseguridad y confianza ene los hogares españoles (Cybersecurity and confidence in Spanish households), ONTSI, available in Spanish at: http://www.ontsi.red.es/ontsi/es/estudios-informes/ciberseguridad-y-confianza-en-los-hogares-españoles
7. Price Waters Coopers (2014): The Global Economic Crime Survey 2014, available at: http://www.pwc.com/gx/en/economic-crime-survey/index.jhtml
8. The International Cyber Investigation Training Academy (2014): Study of the need to establish early warning systems of cybercrime, available in Bulgarian at: http://www.b2centre.com/Бизнесът_трябва_да_се_създаде_система_за_ранно_реагиране_на_киберпрестъпления-c2-ns242_bg.html
9. United Nations Office on Drugs and Crime (2013): Comprehensive Study on Cybercrime. New York: United Nations, February 2013, available at: http://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-CRP05/Comprehensive_study_on_cybercrime.pdf [accessed: 26 April 2015]