Тања МИЛОШЕВСКА

УДК:323.281:[336.746:004.91.056.55
Прегледен труд

ДИГИТАЛНИ КРИПТОВАЛУТИ - НОВ КОНТЕКСТ ЗА ТРАНСНАЦИОНАЛНИ ТЕРОРИСТИЧКИ АКТИВНОСТИ

Кратка содржина

Виртуелните валути, вклучувајќи криптовалути како што е Bitcoin, добија значителна популарност во текот на изминатите неколку години. Целта на трудот е да се согледа дали терористичките организации и терористичките групи во моментов користат криптовалути за финансирање на нивните активности и, ако не, зошто не ги експлоатираат ваквите валути. Криптовалутите се лесни за употреба, безбедни и доколку се користат правилно, можат да го сокријат идентитетот. Последните истражувања тврдат дека терористите ги користат дигиталните криптовалути за финансирање на своите активности. Дали е точно тоа тврдење, и ако е така, до кој степен? И, има ли реални примери кои може да се потенцираат? Особено, факторите што имаат тенденција да ја обесхрабрат употребата содржат континуирана непредвидливост во општествата за криптовалути, соработка меѓу меѓународните полициски служби и разузнавачката заедница и развојот на регулативата и спроведувањето. Прашањето дали терористичките организации ќе ги користат овие системи зависи од достапната технологија, како и од потребите и способностите на овие групи.

Клучни зборови: *ДИГИТАЛНИ КРИПТОВАЛУТИ, ТРАНСНАЦИОНАЛНИ ТЕРОРИСТИЧКИ АКТИВНОСТИ, ДАРК ВЕБ, ТЕРОРИСТИЧКО ФИНАНСИРАЊЕ*

Вовед

Постои голема потреба да се разбере целосниот потенцијал за терористичка употреба на криптовалути, вклучувајќи опции за идентификување и следење на нивната употреба, софистицираност и технолошка способност на терористички групи и потенцијал за такво користење да се зголеми во иднина, со оглед на очекуваниот технолошки развој (Dion-Schwarz at all., 2019).

Сепак, предизвикот поставен од криптовалути се протега надвор од опсегот на биткоинот. Многу нови криптовалути се појавија во изминатите неколку години, вклучително и такви алтернативни валути (altcoins) како што се Omni Layer (MasterCoin), BlackCoin и Monero, кои се промовираат како поприватни и побезбедни од Bitcoin. Zcash е друга криптовалута

која нуди повисок степен на приватност и обезбедува потенцијална можност за користење и трансфер на валута офлајн, што може да го отежни спроведувањето на Законот за откривање незаконски трансакции. Другите криптовалути, вклучувајќи го и Хок, можат да овозможат целосно приватни договори и трансакции на блок-синџирот Ethereum. Како и биткоин, блок-синџирот Ethereum е дистрибуирана компјутерска платформа и оперативен систем (Dion-Schwarz at all., 2019).

Терминологија

Криптовалута означува дигитална валута произведена од јавна мрежа, наместо од која било влада, што користи криптографија за да се осигури дека исплатите се испраќаат и примаат безбедно (Cambridge Dictionary).

Дигиталниот дел се однесува на користење електронски систем што користи бинарен број за снимање звук или зачувување информации и кој дава висококвалитетни резултати (Oxford Learner Dictionary, 2008).

Тероризмот е употреба на насилство за политичка цел. Тероризмот е употреба на насилство врз случајни цивилни цели со цел да се заплашат или да се создаде генерализиран сеприсутен страв заради постигнување политички цели (Yonah, 1976). Дефиницијата за тероризам еволуираше со текот на времето, но неговите политички, религиозни и идеолошки цели практично никогаш не се променија (Sloan, 2006).

Денес, тероризмот се промени единствено во однос на својата димензија, актери, платформа и активности. Тероризмот вклучува акти на киберхакерство, трговија со дрога, киднапирања, тортура, атентати, пропаганда, саботажа, вандализам, воздушни бомбардирања, киднапирања, самоубиствени напади кои вклучуваат чин на насилство кон општеството (Jackson at all, 2011).

Овој труд ја користи организациската теорија за тероризам иницирана од Марта Креншоу (2008). Организациската теорија најмногу ги дискутира целите, дејствијата и внатрешната динамика на терористичката организација. Оваа теорија ја нагласува главната цел на терористичката организација, а тоа е опстанокот што може да се илустрира како државна институција или комерцијално претпријатие. Како одговор на надворешните притисоци, терористичката организација ќе ги менува односно адаптира своите намери преку иновација (Ozdamar, 2008).

Можности на криптовалутите за олеснување на финансирањето на терористичките операции

На терористите им се неопходни значителни финансиски средства за извршување напади и други активности. Доколку терористичките групи се подобро финансирани во целина, може да има почести, поуспешни

и поголеми напади (Acharya, 2009). Постојат неколку причини што ја поддржуваат оваа хипотеза.

Прво, повеќе средства за операции веројатно ќе доведат до зголемено финансирање на структурите што ги овозможуваат овие напади, кои вклучуваат регрутирање и обука на напаѓачи и инспирирање потенцијални осамени волци.

Второ, групите кои се соочуваат со помал монетарен притисок (т.е. оние што се подобро финансирани) исто така може да бидат поподготвени да ризикуваат, како што се поголеми или поризични напади (Shapiro, 2012).

И на крај, а можеби и повеќе спорно, зголемените средства можат да се користат директно за дополнителни и поголеми напади. Можеби е тешко директно да се поврзат зголемените средства со терористички напади, иако во специфични документирани случаи, „литературата често опишува недостиг на готовина како проблем за терористички операции" (Oftedal, 2015).

Дали и како терористичките организации би користеле систем на криптовалута зависи од достапната технологија и нејзините својства, како и од потребите и можностите на организацијата. Поновите криптовалути може да се појават со својства што терористичките организации ги сметаат за попривлечни од оние на моментално достапните криптовалути. На пример, ако идната криптовалута обезбедува подобра анонимност од биткоин за големи трансакции и е пошироко усвоена од Zcash, тогаш терористичките организации би можеле да бидат подготвени да ја користат таа валута за специфични активности. Затоа, важно е да се разгледаат одделни терористички групи за да се анализира што би им требало од криптовалутите и да се споредат тие потреби со својствата на достапните криптовалути.

Биткоинот постојано го користат купувачите и потрошувачите на недозволени добра и услуги на Темната мрежа. Во извештајот под наслов „Терористичка употреба на виртуелни валути: содржана потенцијална закана" се наведува дека терористичките организации ги користеле криптовалутите за да го поддржат опстанокот на нивните организации. На пример, терористичката организација во појасот Газа ги искористи криптовалутите за финансирање на нивните операции, како и членовите и приврзаниците на Исламската Држава во Ирак и Сирија (ИСИС) кои особено ги користеа криптовалутите евидентирани во Индонезија и САД. Забележувајќи понатаму дека значителното и ненадејно губење на нивната физичка територија, како и ширењето на опсегот на воените операции може да го ограничат нивниот пристап и да ги отежнат преместувањата на нивните финансии преку географските области и границите или традиционалната финансиска трансакција наречена хавала која се однесува на физичката финансиска трансакција со користење локален брокер за трансфер на пари помеѓу локации (Ward, 2018). Така, овој феномен потен-

цијално ги охрабрува терористичките организации да ја истражуваат новата технологија што може да ја поддржи нивната способност да ги движат средствата преку криптовалути.

Во трудот се разгледуваат низа примери: конкретно, Ал Каеда и придружните организации, Исламската Држава во Ирак и Сирија (ИСИС), Хезболах, наркотерористички организации и терористи волци самотници. Иако овие групи се разликуваат во нивните цели, нивната потреба за анонимни, безбедни и подготвени насоки на финансирање ги прави криптовалутите со потенцијална вредност за нив. За овие групи, се испитани пет финансиски активности (прибирање финансиски средства, нелегална трговија со дрога и оружје, дознаки и трансфер на средства, финансирање напади и оперативно финансирање) и се процени важноста на криптовалутните својства во олеснувањето на овие активности (Dion-Schwarz at all., 2019).

Постојат различни начини на кои може да се користат виртуелните криптовалути од страна на терористичките групи. Организациите можат да ја користат Темната мрежа за добивање оружје, вклучувајќи традиционално огнено оружје, експлозиви, хемиски или биолошки токсини, плаќајќи ги со виртуелни криптовалути. Виртуелните криптовалути исто така може да олеснат други активности за недозволени приходи од терористички групи; имало на пример виртуелни барања за криптовалути за време на киднапирање за откуп, а киднапирањето за откуп е популарен извор на приход исто така и за терористички организации. Слично на тоа, ако терористичките организации се насочат кон повеќе дигитални напади или кибертероризам, виртуелните криптовалути може да станат покорисни за овие организации бидејќи дозволуваат набавка на „дигитално оружје", како што е малициозен софтвер. Очигледно, виртуелните криптовалути не се клучни за ниту една од овие активности, но тие можат да ги направат овие трансакции полесни од традиционалните плаќања со картички или банкарските трансфери (Entermann and Berg, 2018).

Дополнителен аспект што може да го забрза усвојувањето на виртуелни криптовалути од страна на терористичките групи е конвергенцијата на терористичките и криминалните организации. Терористичките групи веќе долго време користат организирани криминални средства, како што е шверц на тутун, за финансирање на нивните активности и има бројни примери за соработка помеѓу двата типа на групи. Овие се движат од односот на ЕТА со колумбиските наркокартели и олеснувањето на шверцот со кокаин во Европа, до соработката на ПИРА со источноевропските шверцери со луѓе и соработката на Хезболах со мексиканските наркобосови. Во поново време, има зголемен акцент на таканаречената поврзаност криминал-терор, на пример преку движење на лица со криминално минато во терористички мрежи. Најмалку две третини од лицата со оперативна врска со Исламската држава кои извршија напади во Европа и Америка во изминатите неколку години имаа криминално минато (Basra, Neumann,

2017). Постојат докази дека криминалните „вештини“, како што се пристапот до фалсификувани документи и оружје, лесно се користат во нивните нови екстремистички средини. Со оглед на овие случувања, може да биде само прашање на време додека не се извезат виртуелните алатки и тактики на криптовалути што ги користат криминалните синдикати во терористички групи; или дека соработката и трансакциите меѓу терористички и организирани криминалци може да вклучуваат виртуелни криптовалути (Entermann and Berg, 2018).

Овие дигитални криптовалути поседуваат својства како анонимност, употребливост, безбедност, прифаќање, сигурност и волумен. Под анонимност, мислиме на можноста да се скрие и заштити идентитетот на корисникот. Употребливоста се однесува на леснотијата со која корисникот може да спроведува трансакции и да управува со сопствената валута. Безбедноста се однесува на степенот до кој инфраструктурата на криптовалутата обезбедува доверливост, интегритет и точност на трансакциите и корисничките сметки. Под прифаќање, мислиме на степенот до кој валутата е прифатена од корисничката заедница, како и големината на заедницата на корисници. Сигурноста се однесува на брзината и достапноста на трансакциите, како што гледаат корисниците. Конечно, волуменот се однесува на просечната временска збирка на трансакции во инфраструктурата на криптовалутата.

Моментални и идни потреби на терористичките организации за криптовалути

Прашањето дали и како терористичките организации би користеле систем на криптовалута зависи од достапната технологија и нејзините својства, како и од потребите и можностите на групите. Поновите криптовалути може да се појават со својства што терористичките организации ги сметаат за поприврлечни од оние на моментално достапните криптовалути. На пример, ако идната криптовалута обезбедува подобра анонимност од биткоинот за големи трансакции и е пошироко усвоена од Zcash, тогаш терористичките организации би можеле да бидат подготвени да ја експлоатираат таа валута за специфични активности. Затоа, важно е да се разгледаат одделни терористички групи за да се анализира што им е потребно од криптовалутите и да се споредат тие потреби со својствата на достапните криптовалути (Dion-Schwarz at all., 2019).

Сепак, особено со подобрена употребливост, криптовалутите, како што е биткоин, може да бидат привлечни за употреба при прибирање средства, а се појавуваат некои докази дека терористичките организации можат да користат криптовалути за оваа намена (Stalinsky, 2018).

Современите криптовалути се потенцијално многу пофлексибилни, а тоа може да создаде предизвици во финансиското сметководство особено за оние кои се вклучени во спречување компјутерски упади. Областа на

криптовалутите е помалку сигурна, многу подинамична каде иновациите можат да им овозможат на терористичките групи да го заобиколат мониторингот. Од друга страна, тоа е поле каде софистицираноста е важна; перењето пари може да биде потешко да се открие кога го спроведуваат софистицирани актери, но техничките способности на многу терористички групи во моментот не се соодветни за овој вид активност (Dion-Schwarz at all., 2019).

Зголемената употреба на криптовалути на комплементарни и соседни пазари може да укаже на нивната зголемена одржливост меѓу терористичките организации. Некои операции за фалсификување започнаа да користат темни мрежи и постои значителна трговија со украдени кредитни картички и идентитети на овие пазари (Aliens, 2012).

Улога во поширок контекст	Специфични случаи	Опис
Овозможување анонимни финансиски трансакции	Употреба на биткоин преку Tor за анонимност	Додадено ниво на анонимност и претпазливост (DiPiero, 2017)
	Перење пари на криптовалути преку Tumbling услуги	Специфични услуги за перење пари, на пр., преку конвертирање во биткоинси (Dalins et al., 2017)

Постојат неколку недозволени цели на искористување на криптовалутите од терористички организации, како што се набавка на дрога, продажба на наркотици, оружје и дозволување недозволени услуги во Темната мрежа. Покрај тоа, терористичките организации започнаа односно промовираа сопствени донации преку криптовалутите. Може да се заклучи дека криптовалутите може да се претворат во исплата на откуп. Покрај тоа, постојат неколку карактеристики на криптовалути кои обезбедуваат предности за корисниците, односно се подобри од готовина или кредит, размениви за стоки и услуги, конвертибилност и стабилност на вредноста (нестабилност на цената на билансот) (Everette, 2017).

Документирани примери за терористичко стекнување криптовалута

Терористичките мрежи се приспособија на технологијата, вршејќи сложени финансиски трансакции во дигиталниот свет, вклучително и преку криптовалути (The US Department of Justice, 2020).

Врз основа на студијата спроведена од RAND Европа насловена „Зад завесата: недозволена трговија со огнено оружје, распрскувачки материи и муниција на Мрачната мрежа“, постои директна врска помеѓу терористичките напади во Париз и Минхен, како и со оружјето кое било набавено

преку Темната мрежа со криптовалути. Студијата покажува дека имало дваесет и четири пазари на француски и британски криптовалути на Темната мрежа во текот на септември 2016 година, каде што 75 проценти од трансакциите докажале дека реализираат незаконска трговија со оружје (Everette, 2017). Оружјето што го користеле напаѓачите може да биде поврзано со пропагандата на ИСИС која повикувала на ширење поедноставни напади со употреба на возила, огнено оружје, оружје, хемиско оружје и ножеви. Покрај тоа, организацијата поврзана со Ал Каеда, имено al-Sadagah, користела Фејсбук и Телеграм за да ја започне својата финансиска кампања преку биткоин (Malik, 2018).

Во текот на изминатата година, терористичките групи се свртеа кон стекнување и складирање на богатство во виртуелни валути како Bitcoin. Во август 2020 година, Министерството за правда на САД ја објави најголемата заплена до денес на криптоактиви поврзани со терористички групи. Министерството за правда на САД објави дека запленило еквивалент на милиони долари преку повеќе од 300 сметки на криптовалути поврзани со три назначени странски терористички организации во САД имено Хамас, Ал-Каеда и т.н. Исламска Држава. Во 2019 година, военото крило на Хамас започнало кампања за собирање средства на криптовалути преку интернет со помош на алатки за социјални медиуми за поттикнување анонимни донации. Спротивно на популарното верување, анонимноста често поврзана со криптовалути е погрешна именка. Шемата на Хамас последователно се расплетува, со запленети 150 сметки на криптовалути.

Ал-Каеда, исто така, се разграничи со користење алатки за социјални медиуми за да генерира интерес од донатори со цел да ги поддржи нејзините активности во Сирија преку криптовалута. Во случајот на Ал-Каеда, Министерството за правда на САД заплени повеќе од 100 сметки на криптовалути. Интересот на Хамас и Ал-Каеда за криптовалута, соодветно, претходеше на објавата на Министерството за правда на САД, но овој прилив на финансии привлече многу помалку внимание во однос на другите извори на финансирање (IntrelBrief, 2020).

Како и Хамас и Ал-Каеда, ИСИС беше вмешан во соопштението на Министерството за правда во август 2020 година. Слично како на Хамас, така и на Ал-Каеда, лицата поврзани со ИСИС вклучени во шеми на криптовалути не се нови. Во 2017 година, Зообија Шахназ обезбеди 85.000 УСД на ИСИС со тоа што ги зголеми кредитните картички за да купи биткоин, а потоа го претвори Bitcoin во готовина за да ги замагли нелегалните активности. Две години пред шемата на Шахназ, Али Шукри Амин се изјасни за виновен за обезбедување материјална поддршка на ИСИС, покажувајќи им на луѓето како да стекнат и испратат биткоин до групата. Последните напори за криптовалута беа спроведени од Мурат Цакар, хакер на ИСИС (и поврзан со Шахназ) кој создаде веб-страница со наводна продажба на опрема за лична заштита, вклучително и маски за лице N95, заради профит. Со оглед на епидемијата на КОВИД-19 и тешкотиите

поврзани со лични финансиски потфати, случаите во август 2020 година може да претставуваат стожер на организирани терористички групи кон стекнување виртуелни средства. Особено ИСИС веројатно ќе продолжи со напорите за собирање богатство преку операции овозможени преку интернет, од кои некои може да вклучуваат криптовалута (Soufan Center, 2020). На почетокот на 2019 година, бригадите ал-Касам објавија повик на својата страница на социјалните мрежи за донации на биткоин за да ја финансираат својата терористичка кампања. Бригадите ал-Касам потоа го пренесоа ова барање на своите официјални веб-страници, alqassam.net, alqassam.ps и qassam.ps. но, ваквите донации не беа анонимни. Работејќи заедно, агентите на IRS, HSI и FBI ги следеа и запленија сите 150 сметки на криптовалути кои пренесе средства од и од сметките на бригадите ал-Касам.

Во 2020 година, Работната група за финансиска акција (FATF), меѓувладино тело, го потенцираше можното зголемување на терористичкиот интерес за криптовалутата, особено за време на пандемијата КОВИД-19. Во мај, FATF објави извештај во кој се тврди дека пандемијата на коронавирус може да доведе до „зголемување на злоупотребата на онлајн финансиски услуги и виртуелни средства за преместување и прикривање недозволени средства“. Помалку од еден месец по објавувањето на Министерството за правда на САД, FATF објави друг извештај за индикатори со црвен аларм, истакнувајќи дека виртуелните средства може да се користат од финансиери на тероризам и перачи на пари. Индикаторите се движат од уникатни модели на трансакции до профили на географски ризик што може да укажуваат на злоупотреба на виртуелните средства. За единиците за финансиско разузнавање, давателите на услуги за виртуелни средства и финансиските институции, овие индикатори обезбедуваат корисни упатства за спротивставување на употребата на криптовалута од низа недозволени актери. И покрај упатствата на ФАТФ и потегот од август 2020 година на Соединетите Американски Држави за запленување и барање одземање на финансиските средства на Хамас, Ал-Каеда и ИСИС, терористите сè повеќе користат криптовалута за да собираат и складираат богатство. Овој пат е особено веројатен заради веројатното континуирано потпирање на „виртуелно“ деловно работење дури и откако ќе се дистрибуираат вакцините КОВИД-19 во текот на 2021 година. Бидејќи повеќе секојдневни потрошувачи користат криптовалути, можностите за терористите ќе се зголемуваат, бидејќи тие бараат покривање и прикривање на зголемениот обем на вкупните трансакции (Soufan Center, 2020).

Терористите користат виртуелни валути за да избегнат откривање и прибирање финансиски средства. Терористите, како криминалци, користат криптовалути, бидејќи тоа обезбедува иста форма на анонимност во финансискиот амбиент како што е криптирањето за комуникациските системи (Weimann, 2016).

Генерално, употребата на криптовалути треба да се гледа како дел од општата промена кон тероризмот преку интернет (Casadei Bernardi, 2019).

Овој труд покажува дека, доколку се појави криптовалута што обезбедува широка имплементација, подобра анонимност, засилена безбедност и што подлежи на несигурна регулација, тогаш можната корисност на оваа криптовалута, како и потенцијалот за нејзино користење од страна на терористичките организации, ќе се зголеми.

Заклучок

Загриженоста за употребата на криптовалута за да се дозволат терористички активности допрва треба да биде очигледна, но идниот развој на технологиите за криптовалута веројатно ќе има значителна долгорочна последица врз финансирањето на тероризмот. Брзината со која се прифаќаат овие технологии и деталите за тоа кои технологии се користат и како се организирани, се критични несигурности што имаат важни оперативни влијанија. Овој труд предлага регулирање на криптовалутите, заедно со меѓународната соработка меѓу спроведувањето на законот и разузнавачките служби, да бидат императив чекори за да се спречат терористичките организации да користат криптовалути за финансирање на нивните активности.

Безбедноста во опкружувањето на криптовалутите е од умерена до висока позиција за терористичките организации, бидејќи постојните криптовалути се изложени на разновидност на кибернапади.

Сè уште новите врзани валути за кои се претпоставува дека ја унапредуваат безбедноста се предмет на значителен надзор бидејќи со текот на времето се откриваат нови слабости на безбедноста. Кога ги анализираме заемно сите аспекти, вклучително и други значајни фактори како што е конзистентноста и капацитетот на пазарот на криптовалути, ќе откриеме дека ниту една постоечка криптовалута не може да ги реши сите финансиски потреби на терористичките организации.

Литература

Acharya, A. (2009). *Targeting Terrorist Financing: International Cooperation and New Regimes*, New York: Routledge.

Aliens, C (2016). "Darknet Bust: Global Law Enforcement Raids Massive Counterfeiting Organization," *Deep.Dot.Web*, December 17.

Basra R., Neumann P.R. (2017). Development in the crime-terror nexus in Europe, *CTCSentinel*, Vol.10, Issue 9, Combating Terrorism Centre at West Point, USA.

Cambridge Dictionary, "Cryptocurrency," *Cambridge Dictionary.* Available at: https://dictionary.cambridge.org/dictionary/english/cryptocurrency

Casadei B. (2019). Terrorist Use of Cryptocurrencies-A Blockchain Compliance White Paper, Blockchain Consultus, London, United Kingdom.

Crenshaw, M. (2008). Theories of terrorism: Instrumental and organizational approaches, Journal of Strategic Studies, Volume 10.

Dalins, J. at al. (2017). *Criminal motivation on the dark web: A categorisation model for law enforcement.* Digit. Investig.

DiPiero, C. (2017). Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web. U. *Ill. L. Rev.*1267.

Enternmann, E., Willem van der Berg. (2018). *Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?* International Centre for Countering Terrorism, Hague.

Everette J, (2017) *Public-Private Analytic Exchange Program: Risks and Vulnerabilities of Virtual Currency,* Washington: Director of National Intelligence.

IntelBrief (2020). IntelBrief: Terrorists' Use of Cryptocurrency, The Soufan Center, New York, USA, December 10. Available at: https://thesoufancenter.org/intelbrief-2020-december-10/ [Accessed 12 February 2021].

Jackson, R at all. (2011). *Terrorism: A Critical Introduction,* Palgrave Macmillan.

Malik, N. (2018). "How Criminals And Terrorists Use Cryptocurrency: And How To Stop It," *Forbes,* August 31st. Available at: https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and terrorists-use-cryptocurrency-and-how-to-stop-it/#6766399a3990. [Accessed 16 April 2021].

Oftedal, E. (2015). *The Financing of Jihadi Terrorist Cells in Europe*, Norway: Forsvarets Forskningsinstitutt.

Oxford Learner Dictionary. (2008). *Fourth Edition,* China: Oxford University Press.

Ozdamar, O. (2008). "Theorizing Terrorist Behavior: Major Approaches and Their Characteristics", *Defence Against Terrorism Review 1,* No. 2.

Shapiro, J. N. (2012) "Terrorist Decision-Making: Insights from Economics and Political Science," *Perspectives on Terrorism*, Vol. 6, No. 4–5.

Sloan, S. (2006). *Terrorism: The Present Threat in Context*. Oxford: Berg Publishers.

Stalinsky, S. (2018). "The Cryptocurrency-Terrorism Connection Is Too Big to Ignore," *Washington Post*, December 17.

The United States Department of Justice (2020). Office of Public Affairs, *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*, August 13. Available at: https://www.justice.gov/opa/pr/global-disruption-three-terror- finance-cyber-enabled-campaigns. [Accessed 12 February 2021].

Ward, A. (2018). "Bitcoin and the Dark Web: The New Terrorist Threat?" *RAND Corporation,* January. Available at: https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html [Accessed 15 March 2021].

Weimann, G. (2016). "Going Dark: Terrorism on the Dark Web", *Studies in Conflict & Terrorism* 39, 195-206. Available at: http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546. [Accessed 12 February 2020].

Yonah, A. (1976). *International Terrorism: National, Regional and Global Perspectives.* New York: Praeger.