УДК: 343.3::004(4-672EU)
351.86(4-672EU)

Оригинални научни рад

Дипломатија и безбедност
Број 2/2020.
Година III, vol. 3
стр. 77-98.

Михајло Вучић
Институт за међународну политику и привреду, Београд

ИЗАЗОВИ ПРИМЕНЕ РЕСТРИКТИВНИХ МЕРА ЕВРОПСКЕ УНИЈЕ ПРОТИВ САЈБЕР НАПАДА

Сажетак

У раду се обрађује тема рестриктивних мера као инструмента заједничке спољне и безбедносне политике ЕУ, са посебним осврtом на рестриктивне мере против сајбер напада. Истиче се природа режима рестриктивних мера, институционални и процедурални механизми одлучивања, а затим се тежиште анализе помера на посебности рестриктивних мера против сајбер напада. Истиче се преломна улога коју одлука Савета министара ЕУ од 30. јула 2020. има за даљи развој ове области, с обзиром на то да се по први пут у пракси примењују рестриктивне мере против сајбер напада, и то против лица која припадају државним структурама Кине, Русије и Северне Кореје. У раду се анализирају неке препреке практичној примени рестриктивних мера, као што су заштита права погођених лица, приписивање одговорности и усаглашавање одлука између држава чланица. Аутор закључује да у овој области постепено долази до напретка сарадње држава чланица и да се у будућности може очекивати често коришћење рестриктивних мера као средства утицаја на државе које стоје иза сајбер напада.

Кључне речи: рестриктивне мере, санкције, сајбер напади, ЕУ, Савет ЕУ, заједничка спољна и безбедносна политика.

УВОД – РЕСТРИКТИВНЕ МЕРЕ ИЛИ САНКЦИЈЕ?

Рестриктивне мере које Европска унија спроводи у оквиру Заједничке спољне и безбедносне политике (ЗСБП) почињу да се користе као инструмент утицаја Уније у међународним односима од ступања на снагу Уговора у Мастрихту (новембра 1993. године), па до данас, у склопу различитих међународних околности, и у различитим модалитетима деловања, о чему у литератури постоји неколико свеобу-

хватних анализа.[1] Код нас се теорија бавила само посредно овим питањем, више у контексту обавеза у процесу приступања Републике Србије ЕУ[2], или поштовања основних људских права погођених санкцијама Уједињених нација које спроводи Европска унија.[3] До сада, колико нам је познато, нема радова који су се бавили непосредном анализом правног оквира, модалитета коришћења, делотворности и последица режима рестриктивних мера које ЕУ спроводи у оквиру заједничке спољне и безбедносне политике.[4] Појам рестриктивних мера карактеристичан је за мере које предузима ЕУ, док се уопштено гледано овај појам у литератури о међународним односима и међународном праву чешће назива „санкцијама".

Санкције ЕУ имају за циљ да допринесу консолидацији Уније као актера на међународној сцени. Познати недостаци у пројекцији чврсте моћи Уније на спољном плану, пре свега недостатак заједничке војне силе, довели су до повећаног ослањања на санкције као средство притиска за решавање међународних криза. Тренутно, ЕУ има чак 42 активна режима санкција, што је чини другом по реду силом у свету када је у питању ослањање на санкције као средство спољнополитичког утицаја (испред ЕУ су само Сједињене Америчке Државе).[5] Унија се коришћењем санкција диференцира од других актера на међународној сцени који користе неке друге, мање легитимне инструменте утицаја. Истовремено, ефикасном употребом санкција повећава се кредибилитет Уније као велике силе која је способна да управља кризама. Коначно, због једногласне природе процедура за усвајање рестриктивних мера у оквиру заједничке спољне и безбедносне политике, санкције доприносе и повећаној унутрашњој кохезији међу државама чланицама ЕУ. У теорији се истиче како коришћење рестриктивних мера доприноси

1 Види следеће радове: Anthonius W. de Vries and Hadewych Hazelzet, "The EU as a New actor on the sanctions scene", I*nternational sanctions: between words and wars in the global system*, (eds: Peter Wallensteen and Carina Staibano, London, Frank Cass, 2005, pp. 95–107; Clara Portela, *European Union sanctions and foreign policy: when and why do they work?*, Routledge, Milton Park, 2010; Mikael Eriksson, *Targeting peace: understanding UN and EU targeted sanctions*, Farnham, Ashgate, 2011; Francesco Giumelli, *The success of sanctions: lessons learned from the EU experience*, Farnham, Ashgate, 2013; Joakim Kreutz, "Human rights, geostrategy, and EU foreign policy 1989–2008", *International organization*, Vol. 69, No. 1, 2015, pp. 195–217.

2 Види рад на ту тему: Damir Kovačević, Branko Krga, „Osnovni elementi Zakona o međunarodnim restriktivnim merama", *Vojno delo*, br. 3, 2015, str. 155-177.

3 О чему је писао професор Ракић још пре више од десет година. Види: Branko M. Rakić, „Evropski sud pravde između ljudskih prava i borbe protiv terorizma - odnos međunarodnog i evropskog prava", *Anali Pravnog fakulteta u Beogradu*, Vol. 57, Br. 2, 2009, str. 155-185.

4 Аутор је тренутно ментор на изради мастер рада на тему „Рестриктивне мере као инструмент заједничке спољне и безбедносне политике Европске уније", на Факултету за дипломатију и безбедност Универзитета Унион-Никола Тесла, и нада се да ће и тај рад у будућности подстаћи даља истраживања у овој врло занимљивој области.

5 На овом сајту могу се пронаћи подаци о свим тренутно активним и раније постојећим режимима санкција ЕУ, https://www.sanctionsmap.eu/#/main, 10/10/2020.

остварењу идеје о ЕУ као „нормативној сили“.[6] Теорија о „нормативној сили“ тумачи санкције које уводи ЕУ као средства утицаја у циљу промовисања идеја демократије, спречавања ширења нуклеарног наоружања, и подржавања режима изградње мира у пост-конфликтним друштвима.[7] Међутим, теорија о нормативној сили занемарује важан аспекат безбедности, због кога ЕУ такође може имати мотива да уводи санкције лицима која ту безбедност прете да угрозе.

Санкције ЕУ су превазишле традиционалне приступе санкцијама као средству спољне политике који би се могли сажети у следећем ставу: „тешкоће које трпи цивилно становништво државе погођене санкцијама довешће до политичког притиска одоздо ка државним вођама како би се променило њихово непожељно понашање“.[8] Традиционални приступи су одавно у теорији критиковани (с правом) као политички неделотворни и често и контрапродуктивни, јер окрећу цивилно становништво погођене државе против ентитета који намећу санкције, чиме се умањује могућност за постизање политичког решења проблема на који се утиче санкцијама.[9] Генерално гледано, у свету постоји тенденција да се са широко заснованих економских санкција, које без разлике погађају цело становништво санкционисане територије, пређе на циљани приступ, усмерен само на одређена лица, физичка или правна, која су повезана са активностима чија се штетна деловања желе неутралисати санкцијама (такозване „паметне санкције“). У том оквиру и ЕУ намерно своје режиме санкција назива „рестриктивним мерама“, јер се тако наглашава њихово ограничено дејство које погађа само јасно идентификована лица, али и карактер који није казнени као што то сугерише реч „санкција“, већ само ограничавајући за делатности које се желе спречити. Ми ћемо у даљем тексту напоредо користити речи „рестриктивне мере“ и „санкције“, јер мислимо да је чак и у овом ограниченом виду суштина мера које се усвајају казнена према лицима која су наводно одговорна за делатности према којима се санкцијама делује.

У првом делу рада говорићемо уопштено о процедурама усвајања рестриктивних мера у ЕУ. У другом делу ћемо дати посебан осврт на оквир за рестриктивне мере против сајбер напада. У трећем делу ћемо анализирати пример примене рестриктивних мера против сајбер напада у пракси на основу недавне одлуке Савета министара. Затим ћемо се позабавити анализом одређених препрека за ефикасну примену рестриктивних мера у пракси – заштитом права лица која

6 Francesco Giumelli, Fabian Hoffmann, Anna Książczaková, “The when, what, where and why of European Union sanctions“, *European Security*, 2020, стр. 2.

7 Теорију о ЕУ као нормативној сили развио је средином последње деценије прошлог века Томас Рисе-Капен у свом утицајном чланку, види: Thomas Risse-Kappen, “Exploring the nature of the beast: international relations theory and comparative policy analysis meet the European Union“, *Journal of common market studies*, Vol. 34, No. 1, 1996, pp. 53–80.

8 Arne Tostensen, Beate Bull, “Are Smart Sanctions Feasible?“, *World Politics*, Vol. 54, 2002, стр. 375.

9 За критике традиционалних приступа види: Исто, стр. 377.

су погођена мерама, проблемима приписивања одговорности за сајбер напад, и проблемима усаглашавања држава чланица око усвајања јединствене одлуке о рестриктивним мерама. На крају ћемо изнети закључке о свим наведеним питањима.

МЕХАНИЗМИ ОДЛУЧИВАЊА О РЕСТРИКТИВНИМ МЕРАМА У ЕУ

Санкције се у ЕУ усвајају на основу Поглавља II Уговора о Европској унији (Уговор из Лисабона - УЕУ), у коме се садрже посебне одредбе о заједничкој спољној и безбедносној политици. Члан 29. УЕУ је правни основ за одлуке Савета ЕУ којима се усвајају режими санкција. С обзиром на то да одлуке Савета о санкцијама које подразумевају економско-финансијске мере имају непосредне последице на унутрашње тржиште, њихово спровођење у живот је прописано чланом 215 Уговора о функционисању Европске уније. Поред оснивачких уговора, постоје још три акта која су од важности за функционисање општег режима рестриктивних мера. То су најпре „Основна начела“ Савета ЕУ, формулисана још пре доношења УЕУ, 2004. године.[10] Затим, 2018. године Савет је усвојио „Смернице“, низ идеја на основу којих се осмишљавају и спроводе у дело конкретне санкције.[11] У смерницама се наводи да ЕУ прихвата „циљани“ приступ санкцијама, што значи да се мере осмишљавају на начин који минимално утиче на интересе цивилног становништва, а највећи терет санкција сносе она лица која су циљ санкција – појединци одговорни за кршења одређених људских права, политичке партије, или утицајни функционери. Коначно, с обзиром да наметање санкција појединцима представља сложен процес који захтева усаглашавање деловања свих држава чланица како би постигао делотворност, усвојен је и неколико пута ревидиран (са последњом верзијом из маја 2018. године), документ под називом „Најбоља пракса“, који се бави уједначавањем имплементације одлука о санкцијама у свим државама чланицама.[12]

Предлог за усвајање рестриктивних мера може да поднесе Високи представник за спољну политику и безбедност (ВП). На тај предлог могу да уложе коментаре многи органи ЕУ, почевши од Европског савета, до неколико радних група које разрађују област спољне политике и безбедности – KOREPER (комитет сталних представника држава чланица при Савету), Политичко-безбедносни комитет,

10 “Basic Principles on the Use of Restrictive Measures (Sanctions)“, 10198/1/04 REV 1, Brussels, 7 June 2004.

11 “Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy“, 5664/2018, Brussels, 4 May 2018.

12 “Restrictive measures (Sanctions): Update of the EU Best Practices for the effective implementation of restrictive measures“, 8519/18, Brussels, 4 May 2018.

регионалне радне групе и радна група Саветника за спољну политику (RELEX).[13] Наравно, свака појединачна одлука о увођењу санкција, као и свака одлука генерално у области заједничке спољне и безбедносне политике, тражи једногласност у Савету министара. Санкције уобичајено садрже клаузулу о аутоматском подизању након одређеног протека времена – то је обично 12 месеци (мада рок може да варира), осим ако Савет не одлучи да их продужи.[14] Служба за спољне послове ЕУ и Комисија помажу Савету у припреми правних одлука о санкцијама, као и државама чланицама приликом имплементације одлука.

Суд правде ЕУ има такође улогу у процесу примене санкција, и то врло важну, јер је појединцима који су погођени дејством санкција дата могућност да на одлуке Савета уложе жалбу Суду. Треба напоменути да жалбени механизам није изворно предвиђен Уговорима из Лисабона, али се након одлуке Суда у предмету *Кади* (види нешто ниже), број жалби нагло повећао.[15] Суд је у предмету *Кади* одлучивао о оправданости санкција које су Уједињене нације увеле лицима осумњиченим за тероризам, а које су спроводиле ЕУ и државе чланице, дакле не конкретно о директним санкцијама у оквиру ЗСБП. Међутим, случај је привукао пажњу јавности на проблеме кршења људских права који могу да настану спровођењем у живот санкција. Одлуке у оквиру ЗСБП не подлежу судској контроли на исти начин, али теорија се слаже да постоји обавеза органа ЕУ да приликом доношења одлука о санкцијама поштују начела права на правично суђење (право на информисаност, делотворан правни лек, и томе слично), те се Суд правде није устезао да прихвати надлежност за преиспитивање и ових одлука, о чему ћемо говорити нешто касније.

РЕСТРИКТИВНЕ МЕРЕ ПРОТИВ САЈБЕР НАПАДА

Рестриктивне мере до сада увођене у пракси ЕУ састојале су се од забрана продаје и извоза оружја у земље захваћене сукобима или режимима умешаним у масовне ратне злочине, злочине против човечности и геноцид; забрана уласка у ЕУ; дипломатских и економских ограничења, као што су замрзавања имовине, забране обављања финансијских трансакција преко европских пословних банака,

13 О институционалним аспектима спровођења у живот санкција ЕУ види више код Francesco Giumelli, *How EU sanctions work: a new narrative*, Paris, EU Institute for Security Studies, 2013, pp. 10-12.

14 Исто.

15 О судској контроли одлука о санкцијама против лица осумњичених за тероризам, поред раније поменутог Ракићевог чланка (фуснота 3) доста је писала и Кристина Екес, Christina Eckes, "Judicial review of European anti-terrorism measures—The Yusuf and Kadi judgments of the court of first instance", *European law journal*, Vol. 14, No. 1, 2008, pp. 74–92.

трговинска ограничења. У зависности од тога која врсте мере се примењује, разликоваће се и начин имплементације. Ако су у питању економско-финансијске мере, тада искључиву надлежност за њихово спровођење има Савет министара, на основу члана 215. Уговора о функционисању ЕУ, као што смо већ навели. Ако су у питању забране извоза оружја или забране уласка, тада је потребно донети и одговарајуће прописе у државама чланицама, јер је трговина оружјем и контрола територије у надлежности држава чланица.

Нови безбедносни изазови отварају простор и за нове правце деловања рестриктивних мера. Један од главних безбедносних изазова протекле деценије постали су сајбер напади. Сајбер напади су последњих година постали све учесталији, погађају неколико држава чланица ЕУ и на стотине компанија које послују на унутрашњем тржишту. Од 2004. године, седамнаест држава чланица је било изложено утицајима на изборне процесе.[16] 2017. године, вирус "WannaCry" је инфицирао сервере широм ЕУ у до тада невиђеним размерама, оголивши општу рањивост институција и појединаца у нашем дигиталном добу.[17] Само годину дана пре "WannaCry" напада, немачки парламент (Бундестаг) је такође био жртва хаковања, што је изазвало снажну реакцију званичног Берлина, а поједини гласови су захтевали да ЕУ сместа примени режим рестриктивних мера (санкција) према појединцима (руским држављанима) који су наводно стајали иза напада.[18] Вреди поменути и сајбер напад на данско предузеће у области поморског превоза „Мерск" из 2017. године, који је причинио велику штету овом привредном гиганту.[19] Ланац ових догађаја приморао је ЕУ институције да нешто предузму. У склопу тих реакција је усвојена Уредба Савета ЕУ 2019/796, којом је предвиђен механизам санкција (односно рестриктивних мера у терминологији Савета). Уредба наводи низ критеријума за примену санкција, као што су сајбер напади на јавну инфраструктуру, хаковање финансијских институција и употреба уцењивачких вируса (*ransomware* – вируси који заробљавају рачунаре или базе података и потражују откуп за њихово ослобађање), и предвиђају се врсте санкција попут забране уласка у ЕУ и замрзавања имовине у власништву санкционисаних лица која је доступна органима ЕУ.[20]

16 Види извештај Центра за европске политике, бриселског труста мозгова, Centre for European Policy Studies (CEPS), *Strengthening the EU's Cyber Defence Capabilities*, Brussels, 2018, стр. 12.

17 Према подацима Европола, вирус је захватио најмање 75.000 рачунара у 99 земаља. Види: BBC News, "Cyber-attack: Europol says it was unprecedented in scale", 13 May 2017.

18 Kristie Pladson, "Germany proposes first-ever use of EU cyber sanctions over Russia hacking", *Deutsche Welle*, 12/07/2020, Интернет: https://www.dw.com/en/germany-proposes-first-ever-use-of-eu-cyber-sanctions-over-russia-hacking/a-54144559, 10/10/2020.

19 *Strengthening the EU's Cyber Defence Capabilities*, наведено дело, стр. 24.

20 Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ST/7302/2019/INIT, OJ L 129I, 17.5.2019, pp. 1–12.

Рестриктивне мере против сајбер напада су обликоване по узору на правни оквир рестриктивних мера против коришћења и ширења хемијског оружја, при чему су оба режима инспирисана идејом паметних санкција.[21] У поменутом тексту документа Савета министара под називом „Смернице“, истиче се да санкције могу да буду уведене против државе која изводи штетне сајбер активности или сноси одговорност за извођење тих активности од стране неког недржавног актера.[22] Међутим, Уредба Савета 2019/796 не помиње никакво приписивање одговорности за сајбер нападе држави. Циљ је да се делује директно ка лицима која су извела штетне активности, како би се она онемогућила да то чине убудуће, а не да се утврђује одговорност државе за понашање тих лица, што је по нама реалан и оправдан приступ. У супротном би режим санкција практично прерастао у реторзију чије су границе дозвољености у међународном праву упитне.[23]

Рестриктивне мере се примењују против сајбер напада који долазе изван територије ЕУ, било да погађају њене држављане, органе Уније или држава чланица, или неку трећу државу или међународну организацију.[24] Израз „долазе изван територије ЕУ“ може да подразумева неколико различитих ствари: 1) да напади започињу или се одвијају изван територије ЕУ; 2) да се напади изводе од стране правног или физичког лица, тела или ентитета који има седиште изван ЕУ или делује изван ЕУ, односно да се напади изводе уз подршку, под контролом или координацијом таквог лица; 3) да напади користе инфраструктуру која је лоцирана изван ЕУ.[25] Ти напади морају да представљају претњу по интересе ЕУ, што може да значи следеће: 1) упад у информационе системе; 2) ометање рада информационих система; 3) ометање или пресретање података; 4) штетни утицај на критичну инфраструктуру или услуге које су неопходне за вршење социјалних функција државе (нпр. у енергетском или транспортном сектору); 5) штетни утицај на складиштење и обраду поверљивих државних података; 6) штетни утицај на државне тимове за реаговање у ванредним ситуацијама.[26]

---

21 Види релевантну одлуку Савета о режиму санкција против хемијског оружја: Council Decision (CFSP) 2018/1544 of 15 October 2018 concerning restrictive measures against the proliferation and use of chemical weapons, OJ L259/25.

22 “Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy“, 5664/2018, Brussels, 4 May 2018.

23 За расправу о односу санкција ЕУ и реторзије као института општег међународног права види рад Stjepan Novak, „Uvodno o sankcijama Evropske Unije“, *Zagrebačka pravna revija*, Vol. 2, No. 1, 2013, стр. 65.

24 Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ST/7302/2019/INIT, OJ L 129I, 17.5.2019, pp. 1–12.

25 Исто.

26 Исто.

ОДЛУКА САВЕТА ЕУ ОД 30. ЈУЛА 2020.

Протеклог лета забележен је преломни тренутак у режиму примене рестриктивних мера као инструмента спољне политике Европске уније. Наиме, 30. јула 2020, Савет ЕУ је по први пут у оквиру заједничке спољне и безбедносне политике (ЗСБП) усвојио циљане рестриктивне мере против шест кинеских и руских држављана, два правна лица из ове две земље и трећег правног лица са седиштем у Северној Кореји.[27] Разлог усвајања мера била је умешаност наведених лица у радње или покушаје радњи сајбер напада значајног интензитета против саме ЕУ или њених држава чланица. У питању су сајбер напади који су имали ширег одјека у јавности и постали познати под именима "WannaCry"[28], "NotPetya"[29], "Operation Cloud Hopper[30]", као и покушај напада на Организацију за забрану хемијског

27 Види одлуку Савета ЕУ, Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ST/9564/2020/INIT, OJ L 246, 30/07/2020.

28 Напад вируса "WannaCry ", који је погодио сервере британске националне здравствене службе и узроковао милионе фунти губитака у приватном здравственом сектору, извела је севернокорејска хакерска група „Lazarus", према писању Њујорк Тајмса повезана са владом Северне Кореје. Види: Nicole Perlroth, "More Evidence Points to North Korea in Ransomware Attack", *The New York Times*, May 22, 2017.

29 "NotPetya"се сматра најразорнијим сајбер нападом у историји, према речима извршног директора компаније "Cisco", Крега Вилијамса вирус "NotPetya" се размножавао брже него било који други компјутерски вирус у историји. Вирус је првобитно циљао сервере јавног предузећа за производњу и дистрибуцију електричне енергије у Украјини и био је искоришћен као сајбер оружје у оквиру рата који се води у Украјини. Међутим, брзи степен преношења вируса довео је до угрожавања безбедности у многим земљама Европе, па чак оштетио и сервере „Росњефта". С обзиром да је за употребу вируса окривљена руска војна обавештајна служба ГРУ, види се колико је коришћење сајбер оружја непредвидиво у својим последицама. Укупна штета због ометених пословних операција од деловања вируса процењена је на око 10 милијарди долара. Види: Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Security*, 22/8/2018.

30 Два званичника у Министарству националне безбедности Народне Републике Кине доведена су у везу са низом сајбер напада на европске компаније у области технолошких услуга (између осталих и шведски „Ериксон") у периоду између 2014. и 2017. године. Напади су циљали сервере мултинационалних компанија лоциране на територији ЕУ како би украли на њима ускладиштене податке корисника услуга ових компанија, међу којима су се налазиле бројне пословне и државне тајне. Према изјавама европских званичника, цела операција је спровођена у циљу повећања конкурентности кинеске привреде. Види: Jack Stubbs, Joseph Menn and Christopher Bing, "Inside the West's failed fight against China's 'Cloud Hopper' hackers", *Reuters Investigates*, 26 June 2019.

оружја (OPCW).[31]

На тај начин је по први пут примењен у пракси режим сајбер санкција усвојен Уредбом Савета 2019/796. Треба напоменути како је Уредба 2019/796 разрадила ранији стратешки документ Савета под именом „Приручник сајбер дипломатије".[32] Приручник је замишљен као одговор на претње међународном миру и безбедности које настају у сајбер простору. Поред уобичајених дипломатских алата, као што су превентивне мере, мере сарадње и стабилизације, овај приручник даје могућност Савету да наметне циљане санкције државама или недржавним актерима у циљу одговора на или спречавања сајбер-напада, чак и када штетне сајбер активности не представљају акте противне међународном праву, али су по оцени Савета непријатељске према ЕУ или државама чланицама.[33] Савет тумачи циљане рестриктивне мере као мере које немају везе са утврђивањем одговорности неке државе за сајбер нападе, сматрајући да је то суверена политичка одлука коју је свака држава чланица слободна да донесе за сваки конкретан случај. На тај начин се мерама одузима природа накнаде као инструмента међународног права који има за циљ да на основу утврђене одговорности државе за противправни акт исправи нанету штету оштећеној држави. Циљ рестриктивних мера у сајбер простору које усваја ЕУ је утицање на промену политике државе која се циља мерама, или на њене органе, или на правна и физичка лица која имају њено држављанство, или делују са њене територије.

Међутим, како је истакнуто у литератури, „пракса показује да је највећи број сајбер напада који су узроковали тешке последице (Stuxnet, WannaCry, NotPetya) изведен на захтев и уз подршку државних органа, а не неке случајне скупине

31 Organization for the Prohibition of Chemical Weapons, међународна организација са седиштем у холандској престоници Хагу, која спроводи у живот одредбе Конвенције о забрани хемијског оружја, њени циљеви су елиминисање коришћења и претњи коришћењем хемијског оружја, зарад усмеравања хемијске технологије ка циљевима мира, напретка и безбедности, види вебсајт организације на https://www.opcw.org/, 10/10/2020. За напад на седиште OPCW-а су окривљена четворица агената Војно-обавештајне службе Руске федерације (ГРУ) који су због тога 2018. године депортовани из Холандије. На листи санкција Савета нашао се и такозвани „Главни центар за посебне технологије", одељење ГРУ које се специјализовало за хакерске операције, а повезивано је и са NotPetya нападима.

32 Cyber Diplomacy Toolbox, види текст закључака Савета ЕУ о оквиру за заједничко дипломатско реаговање ЕУ на штетне сајбер активности (Приручник сајбер дипломатије), Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), Brussels, 7 June 2017, 9916/17, Интернет, https://data.consilium.europa.eu/doc/document/ ST-9916-2017-INIT/en/pdf, 10/10/2020.

33 Види Смернице Савета ЕУ за имплементацију оквира за заједничко дипломатско реаговање ЕУ на штетне сајбер активности, Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, Brussels, 9 October 2017, 13007/17, Интернет, https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf, 10/10/2020.

хакера".[34] Према томе, у пракси је врло магловита линија разграничења између приписивања одговорности држави и циљаних мера којима се погађају појединци иза којих вероватно стоји државна организација. Подсетили бисмо да ЕУ има и Директиву о нападима на информационе системе, чије одредбе предвиђају и казне за лица која изврше кривично дело против сајбер безбедности, а да притом нису повезана са државним структурама.[35] У одлуци Савета од 30. јула 2020, поменута правна и физичка лица су подвргнута режиму рестриктивних мера јер су наводно одговорна за сајбер нападе или покушаје сајбер напада, или су дала подршку или олакшала извођење тих напада. Мере забрањују наведеним лицима да уђу на територију ЕУ, замрзавају сву њихову имовину и финансијска средства која су доступна органима ЕУ и забрањују било какво финансирање рада активности ових лица.

ЗАШТИТА ПРАВА ЛИЦА ПОГОЂЕНИХ РЕСТРИКТИВНИМ МЕРАМА

Мере које погађају наведена лица имају значајне последице по остварење њихових основних људских права, пре свега права на имовину, слободу кретања и привредног пословања. Такође, начин усвајања мера може да повреди процесна права на правично суђење и делотворни правни лек. Коначно, уколико дође до грешке у приписивању одговорности за сајбер напад неком физичком лицу, поставља се и питање кршења његовог права на приватност података. Ово су релевантна питања, јер ЕУ гарантује да њени акти неће кршити основна људска права која чине саставни део њеног правног поретка. Суд правде ЕУ је у случају *Кади I* истакао како судови ЕУ морају да врше контролу над законитошћу аката органа ЕУ у светлу основних људских права која чине правни поредак ЕУ.[36] У предмету

34 Yuliya Miadzvetskaya, "Challenges of the Cyber Sanctions Regime under the Common Foreign and Security Policy", *Security and Law*, eds. Anton Vedder, Jessica Schroers, Charlotte Ducuing, Peggy Valcke, KU Leuven Centre for IT & IP Law Series, Volume 7, 2019, стр. 281.

35 Види: 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, *Official Journal of the European Union*, L218/8. Циљеви Директиве су да изједначи кривичноправне прописе држава чланица у области напада на информационе системе, тако што поставља минималне стандарде у погледу дефиниције кривичних дела и пратеће санкције, као и да унапреди сарадњу између надлежних органа, полиције и других посебних органа гоњења држава чланица, као и специјалних агенција и тела Уније у области безбедности – Евроџаст (Eurojust), Европол (Europol), Европски центар за сајбер криминал и Европска агенција за мреже и информациону безбедности.

36 Суд правде ЕУ, Пресуда Великог већа од 3. септембра 2008: Judgment of the Court (Grand Chamber) 3 September 2008, ECLI:EU:C:2008:461, Cases C-402/05 P and C-415/05 P, пара. 326. Интернет: http://curia.europa.eu/juris/document/document.jsf?text=&docid=67611&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1976841, 10/10/ 2020.

Кади II, Суд је појаснио да лица која су погођена актима ЕУ имају право да буду саслушана, да добију приступ подацима који их терете, уз легитимна ограничења тог приступа уколико су подаци поверљиви.[37] Суд је разрадио и појам права на правично суђење у овом контексту: „подразумева се да дато лице мора да буде у стању да утврди разлоге због којих је одлука у вези са њим донета, било тако што ће само прочитати одлуку или ће на његов захтев разлози бити објављени, без ограничења права надлежног суда да захтева од датог органа да открије ту информацију, тако да се том лицу омогући да брани своја права у најбољим могућим условима и да одлучи, уз пуну свест о релевантним чињеницама, да ли има сврхе да се жали надлежном суду, као и да би надлежни суд могао у потпуности да испита законитост дате одлуке".[38]

Дакле, одлука да се неком лицу наметну циљане рестриктивне мере подлеже јасним критеријумима, који се процењују од случаја до случаја, и морају бити испуњени да би се неко лице ставило на листу санкционисаних лица, као и да би се са те листе уклонило. Штавише, Савет ЕУ је обавезан да образложи своју одлуку на основу члана 296. Уговора о функционисању ЕУ, у коме се наводи да образложење не обухвата само правни основ донете мере, већ и за сваки појединачни случај наведене конкретне и прецизне разлоге зашто надлежни органи сматрају да неко лице треба да буде подвргнуто режиму рестриктивних мера.[39]

Врло је тешко ускладити захтев за прецизним и конкретним доказивањем разлога зашто се неко лице ставља на листу санкционисаних лица са тешкоћама иоле извеснијег приписивања сложених и готово по правилу анонимних случајева сајбер напада. У нашем посматраном случају, Савет наводи да су сајбер напади могли да буду приписани санкционисаним лицима на основу анализе техничких података и прикупљених информација из свих извора, у које спадају и могући мотиви нападача.[40] Међутим, ако би се ти подаци, а поготово извори прикупљених информација објавили, дошло би до угрожавања безбедности и ЕУ и њених држава чланица. Према томе, онај део пресуде у предмету *Кади* који се односи на право на доступност доказа не може да се посматра као апсолутно важећи у контексту сајбер напада. Право на доступност доказа се трансформише у тест одмеравања супротстављених интереса права на правично суђење окривљеног и интереса јавне безбедности. Уколико интереси јавне безбедности превагну, на на-

37 Суд правде ЕУ, Пресуда Великог већа од 18. јул 2013: Judgment of the Court (Grand Chamber) 18 July 2013, ECLI:EU:C:2013:518, Cases C-584/10 P, C-593/10 P and C-595/10 P, пара. 99, Интернет: http://curia.europa.eu/juris/document/document.jsf?text=&docid=139745&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1977120, 10/10/2020.

38 Исто, пара. 100.

39 Општи суд ЕУ је потврдио важност члана 296. у контексту рестриктивних мера у предмету Il Su-Kim & KNIC, Judgment of the General Court (Third Chamber), 14 March 2018, ECLI:EU:T:2018:13.

40 Одлука Савета од 30. јула 2020, нав. дело.

ционалним судовима је да одлуче да ли су ти интереси у сваком поједином случају оправдали ограничење права на правично суђење. То значи да лице које се нађе на листи санкционисаних лица очекује дуги пут кроз правосудне органе ЕУ и држава чланица уколико жели да сазна стварне разлоге због којих се на листи нашло.

ПРОБЛЕМ ПРИПИСИВОСТИ

Приписивост је појам који се односи на процес одређивања учиниоца неког акта. У случају сајбер напада, приписивање је процес повезивања конкретних сајбер операција са лицима која су операције непосредно изводила, контролисала непосредне извршиоце, или руководила целокупним нападом. Да би се санкције увеле неком лицу потребно је да се то лице доведе у везу са актом који се санкцијама жели казнити, односно чије се понављање у будућности жели спречити. Након председничких избора у САД 2016. године поставило се питање уплива руских хакера и тролова на изборну кампању, па чак и крајње резултате избора. Портпарол председничке администрације Руске Федерације, Димитри Песков, одбацио је том приликом све наводе Централне обавештајне агенције (ЦИА) којим су истински постојећи акти хаковања мејлова демократских председничких кандидата и манипулисања изборном вољом одређених бирача преко друштвених мрежа приписани Русији.[41] Званични Кремљ је стао на становиште да се у тим ситуацијама или изнесу чврсти докази или се уопште ништа и не износи у јавност.[42]

У начелу, приписивост као процес одређивања учиниоца сајбер напада зарад увођења санкција се налази негде између ова два става. Структура интернета и релативна анонимност његових корисника су велике препреке неком формалноправном доказивању одговорности. Европска комисија је препознала овај проблем и позвала на реформу ИП (IP) адреса како би се олакшала истрага терористичких група које уживају у некажњивости због анонимности онлајн саобраћаја.[43] Ту иницијативу нису пратиле неке конкретне мере и чини се да за сада не постоји технички начин којим би се ограничила анонимност онлајн саобраћаја. Ипак, приписивост захтева извођење одређених уверљивих доказа, степен уверености државе која приписује одређени акт у постојање одређених чињеница који може да ужива поверење јавног мњења и других држава. Без тог степена уверености,

41 Песков је једноставно описао те наводе као „бесмислице“, David Filipov, “Kremlin calls talk of Russian interference in U.S. elections ‘absolute nonsense’“, *The Washington Post*, December 13, 2016.
42 Laura Smith-Spark, “Russia challenges US to prove campaign hacking claims or shut up“, *CNN World*, December 16, 2016.
43 *Cyber Diplomacy Toolbox*, нав. дело, стр. 13.

свака акција која би уводила санкције или предузимала друге противмере не би могла да користи угледу државе која мере примењује. „Приручник сајбер дипломатије“ наводи следеће оријентационе критеријуме: „да би се одређена сајбер активност везала за неку државну територију и за лица која стоје иза те активности, и да би се утврдило саучесништво између хакера појединца и државних структура, потребно је савесно прикупити информације из свих расположивих извора, уз коришћење техника праћења и узимајући у обзир могући интерес који би потенцијални учинилац могао да има за извршење сајбер напада“.[44]

Приписивање је процес који подједнако има везе са техничким аспектима коришћења интернета и правним институтима доказивања. У појединим ситуацијама је врло лако приписати напад одређеном лицу, као што је то био случај са приписивањем сајбер напада на компанију „Сони“ Северној Кореји.[45] У анализу је потребно убацити геополитичке факторе (ко је коме ривал, непријатељ?), правну способност систематског тумачења појединачних доказа и здраву логику. Рецимо, када је “Stuxnet“ вирус напао Иран и оштетио ирански нуклеарни програм, искористивши мане у систему на врло информисан начин коришћењем метода које су указивале на постојање знатних ресурса у позадини операције, Иран је убрзо закључио да иза дате операције морају да стоје његови традиционални непријатељи, САД и Израел, државе које су једино и могле логистички да организују операцију таквог обима, да располажу до те мере прецизним обавештајним подацима о иранском нуклеарном програму, и које су имале стратешки интерес да спрече Иран да дође до нуклеарног оружја.[46]

Када ЕУ покушава да припише сајбер напад неком лицу, осим техничких и правних препрека у процесу приписивања, појављују се и сложене политичке дилеме усаглашавања 27 држава чланица око заједничког става о приписивости. Државе чланице су слободне да припишу сајбер напад лицу за које применом правно-техничких мера утврде да стоји иза њега.[47] Мисироли истиче како државе чланице информације о конкретном сајбер нападу често задржавају за себе као строго поверљиве.[48] Уколико би државе изашле у јавност са целокупним приказом својих извора из којих прикупљају информације и форензичких метода којима долазе до доказа, њихова безбедност би могла да буде додатно угрожена. Са друге стране, ако не пруже довољно доказа, окривљени лако могу да одбаце наводе и у

44 *Cyber Diplomacy Toolbox*, нав. дело, стр. 13.

45 Напад је успео да омете премијерно приказивање филма „Интервју“ у биоскопима, чија је тема фиктивно убиство Ким Џонг Уна, лидера ове државе, Timothy B. Lee, “The Sony hack: how it happened, who is responsible, and what we've learned“, Vox, December 17, 2014.

46 Kristen Eisencher, “Cyber Attribution Problems—Not Just Who, but What“, *Just Security*, December 11, 2014.

47 *Cyber Diplomacy Toolbox*, наведено дело, стр. 13.

48 Antonio Missiroli, “The Dark Side of the Web: Cyber as a Threat“, стр. 142.

међународном јавном мњењу добију медијски рат. Такође, у свету сајбер активности не постоје међународне организације попут Организације за забрану хемијског оружја које би могле да пруже непристрасна вештачења. Све су то разлози због којих правни оквир сајбер санкција ЕУ разликује питање циљаних рестриктивних мера од приписивања одговорности за сајбер напад одређеној држави. Као што смо већ навели, примена рестриктивних мера у вијећењу Савета министара није истовремено и приписивање; приписивање остаје суверена политичка одлука коју свака држава чланица може да донесе у сваком појединoм случају. Постоји, дакле, јасна граница између одговорности лица које се погађа рестриктивном мером и одговорности државе чија се улога у сајбер нападу види из доказа на којима је заснована одлука о рестриктивној мери. Чини се да је ова граница морала да буде постављена како би се олакшала процедура за усвајање одлука у области рестриктивних мера, која захтева једногласност, и сходно томе мукотрпно усаглашавање понекад врло супротстављених ставова држава чланица.

УСАГЛАШАВАЊЕ ОДЛУКА О РЕСТРИКТИВНИМ МЕРАМА

Главна препрека глатком функционисању заједничке спољне и безбедносне политике ЕУ је процес одлучивања који захтева компликовани механизам дипломатских преговора ради постизања једногласја. Уз сталне унутрашње поделе међу државама чланицама, та препрека је понекад непремостива.[49] Још од Уговора у Мастрихту, ЗСБП је другачија политика у односу на остале ЕУ политике, такозвани хоризонтални стуб деловања у коме нема ничег наднационалног, већ се све своди на сарадњу међу владама држава чланица.[50] Разлике у политичким и економским интересима држава чланица могу да поремете процесе одлучивања који су у интересу ЕУ као целине. Неке државе чланице могу да по појединим питањима заузму тврђе, неке мекше ставове. Примера је много, подсетимо овом приликом на епизоду током једног од самита ЕУ - Русија, када су институције ЕУ осудиле руске војне операције у Чеченији, али је тадашњи италијански премијер Силвио Берлускони заузео афирмативан став према праву Русије да се обрачунава са чеченским сепа-

49 Изласком Велике Британије из ЕУ, донекле је олакшано постизање сагласности, с обзиром на добро познате разлике у ставовима које су Британци имали у односу на потребу јединственог наступа ЕУ у осетљивим спољнополитичким питањима у односу на Француску или Немачку, о чему сам писао у ранијем броју овог часописа, види Михајло Вучић, „Брегзит – Преговори и могући исходи", *Дипломатија и безбедност*, Год I, Vol. 2, 2018, str. 173-176.

50 За разлику од хоризонталног стуба, вертикални стуб деловања у који спада унутрашња безбедност и бројна економска питања одликује се превагом ЕУ институција у односу на суверенитет држава чланица, Paul James Cardwell, "The Legalisation of European Union Foreign Policy and the Use of Sanctions", *Cambridge Yearbook of European Legal Studies*, Vol. 17, 2015, стр. 300.

ратистима.[51]

Према томе, дешава се да у појединим случајевима државе чланице дају предност одржавању добрих односа са трећим државама у односу на доследну спољну и безбедносну политику. Као последица се јавља пренос одлуке о мерама са нивоа заједничког деловања ЕУ на билатерални однос државе погођене сајбер нападом према држави за коју постоје докази да стоји иза напада. Тако је Велика Британија јавно приписала сајбер нападе против одређених провајдера услуга одржавања система информационих технологија групи „АПТ 10“, коју је повезала са Министарством државне безбедности Народне републике Кине.[52] Влада Велике Британије је ступила у преговоре са кинеским властима како би се пронашло решење, али су се у међувремену сајбер напади наставили, што доводи до питања: да ли је билатерални одговор довољно ефикасно решење? Свакако да јединствен став ЕУ у осуди одређене државе може да повећа шансе да ће та држава изменити понашање у будућности.

Осим тога, државе чланице ЕУ се разликују и по проценама ризика, јер нивои дигитализације и сајбер капацитета њихових друштава нису уједначени. Обавештајне агенције држава чланица због тих разлика могу да дођу до неуједначених закључака о чињеничном стању. Зато су многе државе врло опрезне према заједничком усвајању рестриктивних мера, јер би грешка у приписивању сајбер напада могла да има тешке последице по њихов углед и односе са државом која би била окривљена. Италија је била међу државама које су се снажно противиле усвајању правног оквира за рестриктивне мере против сајбер напада[53]; мислимо да је један од главних разлога била њена сарадња са Кином у оквиру иницијативе „Појас и пут“.[54] Белгија, Финска и Шведска су заговарале такозвани „постепени приступ“, у коме би санкције биле само крајње средство.[55] У трећој групи били су Велика Британија, Француска, Естонија, Холандија, Румунија, Словачка, Летонија, Литванија и Пољска, које су подржале у потпуности увођење рестриктивних мера у сајбер простору.[56] Ове разлике се усаглашавају дипломатским преговорима, који

51 Види више о томе у књизи Anna-Sophie Maass, E*U-Russia Relations, 1999–2015: From courtship to confrontation*, Routledge, London, 2016, стр. 46.

52 “Press release: UK and allies reveal global scale of Chinese cyber campaign“, *GOV.UK*, 20/12/2018, Интернет:https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign,10/10/2020.

53 “Italy resists EU push to impose sanctions over cyberattacks“, *Euractiv*, 15 October 2018.

54 Италија је марта 2019. године постала и званичан партнер Кине у оквиру иницијативе „Појас и пут“. О неуједначеном ставу држава чланица ЕУ према Кини, када је у питању иницијатива „Појас и пут“, писао сам у недавно објављеном чланку: Mihajlo Vučić, “European Union integration and the Belt and Road Initiative: A Curious case of Serbia“, *Međunarodni problemi*, Vol. LXXII, No. 2, 2020, стр. 342-343.

55 “Italy resists EU push to impose sanctions over cyberattacks“, *Euractiv*, 15 October 2018.

56 Исто.

су исцрпљујући и дуго трају. Не охрабрује чињеница да је једва усвојен правни оквир, а да ће за сваку појединачну одлуку опет бити потребно усаглашавање. Прелазак на гласање квалификованом већином би олакшао умногоме читав процес. Председница Европске комисије, Урсула фон дер Лејен, заложила се неколико пута до сада да се у области санкција за повреде људских права уведе већинско одлучивање[57], те сматрамо да са даљим растом опасности од сајбер напада можда дође и до сличних иницијатива у овом домену.

На крају, чак и када се колективна одлука усвоји, она често буде недоречена, како би се избегла могућа повезивања осуђених сајбер напада са конкретним државама. Велика Британија и Данска су одмах јавно приписале "NotPetya" сајбер напад руском ГРУ, а поједине државе чланице након тога су издале саопштења којима их подржавају. Међутим, првобитни закључци Савета ЕУ из априла 2018. године су се свели на „осуду штетне употребе информационих и комуникационих технологија"[58]. Приликом напада на седиште Организације за забрану хемијског оружја, Велика Британија и Холандија су одмах указале на умешаност Русије у напад и заговарале одлучну акцију. Међутим, Италија и Француска су оклевале да јавно прогласе Русију одговорном.[59] На нивоу ЕУ институција је такође дошло до размимоилажења у ставовима. Тадашњи Председник Европског савета Доналд Туск издао је заједничко саопштење са Председником Комисије Јункером и Високом представницом за спољну политику и безбедност Могеринијевом у коме су приписали одговорност за напад Русији,[60] док Европски савет није постигао сагласност око тог питања, и само је издао саопштење у коме је општим изразима осудио непријатељски сајбер напад према OPCW.[61]

Управо је због ове недореченості у претходним примерима врло битно за даљи развој рестриктивних мера ЕУ у сајбер простору то што је одлукама Савета министара од 30. јула 2020. несумњиво изражен став око природе сајбер напада на OPCW и "NotPetya", те су лица за која се сматра да су одговорна за напад кажњена. Сама одговорност државе није утврђена, нити је то циљ рестриктивних мера онако

57 Последњи пут то је учинила у вези са догађајима у Белорусији око намештања избора и несразмерне примене физичке силе према демонстрантима, док се у ранијим приликама оглашавала око стања људских права у Русији и Турској. Види: By Alexandra Brzozowski, Vlagyiszlav Makszimov, "EU diplomacy needs more courage to address Russia, Turkey, new White House", *Euractiv*, 16 September 2020.

58 "Italy resists EU push to impose sanctions over cyberattacks", *Euractiv*, 15 October 2018.

59 Lauren Cerulus, "Russia dodges bullet of EU sanctions on cyber — for now", *Politico*, 22/10/2018.

60 "Joint statement by Presidents Tusk and Juncker and High Representative Mogherini on Russian cyber attacks", *European Council*, 04/10/2018, Интернет: https://www.consilium.europa.eu/en/press/press-releases/2018/10/04/joint-statement-by-presidents-tusk-and-juncker-and-high-representative-mogherini/, 10/10/2020.

61 Према: Yuliya Miadzvetskaya, "Challenges of the Cyber Sanctions Regime under the Common Foreign and Security Policy", нав. дело, стр. 287.

како их је Савет конципирао, али се с обзиром на држављанство и структуре из којих потичу циљана лица може јасно видети ко би могао да стоји иза њих. Ако ЕУ жели да говори једним гласом на међународној сцени и да ефикасно користи рестриктивне мере као средство спољнополитичког утицаја, одлуке као што је ова од 30. јула 2020. у будућности морају у потпуности да истисну противречне и недоречене ставове о којима смо говорили у овом одељку.

ЗАКЉУЧАК

Рестриктивне мере су одговор на претње које угрожавају ЕУ, или вредности за које се она залаже, а долазе изван њене територије. ЕУ се у пројекцији свог спољнополитичког утицаја веома ослања на овај инструмент, не само зато што не располаже тврдом моћи, већ што гради свој идентитет као актера у међународним односима на поштовању норми понашања. Рестриктивне мере су тако санкција за кршење норми које ЕУ сматра важним за исправно функционисање међународних односа. Међутим, да би се избегла повезаност појма санкција са казненом природом овог појма, у жаргону заједничке спољне и безбедносне политике ЕУ је уведен појам рестриктивна мера. Она нема за циљ да утврди одговорност неке државе за повреду норми, нити да без дискриминације погађа становништво неке територије, већ жели да осуди и казни појединце који стоје иза кршења норми и да утиче да се то кршење у будућности више не понови.

Рестриктивне мере у сајбер простору су настале као последица све већих безбедносних изазова који се јављају због учесталих сајбер напада. Одлуком Савета ЕУ од 30. јула 2020. је по први пут примењен овај механизам у пракси против држављана из три државе који су извели низ тешких сајбер напада на територију држава чланица ЕУ, институције ЕУ и међународне организације са седиштем на њеној територији. Иако рестриктивне мере не утврђују одговорност држава у чијим безбедносним структурама на основу изнетих доказа делују циљани појединци, јасно је да се њима посредно утиче на понашање ових држава да прекину да контролишу или подржавају сличне сајбер нападе у будућности.

У раду је анализирано и неколико проблема са којима се рестриктивне мере у сајбер простору могу сусрести у даљој примени у пракси. Проблеми поштовања права лица погођених мерама, приписивања одговорности, и усаглашеног деловања држава чланица су појединачно анализирани. Увођење рестриктивних мера захтева спровођење одређеног доказног поступка, који није еквивалентан доказивању кривице пред судом, али мора да буде кредибилан како би мере постигле циљ – утицај на треће државе и међународно јавно мњење да их прихвате као оправдане. У супротном, могуће је да државе које стоје иза окривљених лица добију инфор-

мациони рат ако успеју да обезвреде слабо засноване доказе. Такође, рестриктивне мере, као што им само име каже, ограничавају у великој мери људска права погођених лица, која имају право на судску заштиту пред Судом правде ЕУ, који може да поништи конкретне мере ако утврди да су неоправдане. Проблеми код приписивања одговорности настају као последица сложеног правно-техничког процеса територијализације и персонализације сајбер напада, односно везивања за одређену територију активности којима је извршен сајбер напад и идентификације анонимних хакера. Коначно, државе чланице морају да усагласе ставове око приписивања и доказа који стоје иза њега, како би се усвојила јединствена одлука о санкцијама. Различити политички и економски интереси држава чланица, као и различит ниво оспособљености обавештајних служби да изведу доказе, односно процене ризике, доводе до могућности да се за исти напад окриве различити актери. Како немају све државе чланице једнаке интересе, некада се и за очигледне ствари појављују различита гледишта, јер су поједине чланице спремне да „зажмуре“ пред доказима да не би кариле односе са државом која стоји иза напада.

Имајући све наведено у виду, одлука Савета од 30. јула 2020. којом се уводе рестриктивне мере за 6 лица окривљених за низ тешких сајбер напада представља веома велико достигнуће. Одлука је заснована на кредибилним доказима који су прикупљани неколико година удруженим радом обавештајних служби и техничких експерата држава чланица и заједничких ЕУ институција. Око одлуке је постигнута сагласност свих чланица, иако је за исте догађаје у прошлости постојало размимоилажење у тумачењу не само међу лидерима различитих чланица, већ и међу самим ЕУ институцијама. Приписивање је извршено само у односу на индивидуалну одговорност, али је због положаја и улоге коју лица имају у државним структурама јасно да она не би могла да изведу нападе на своју руку, чиме се шаље посредна порука тим државама да ЕУ неће седети скрштених руку и посматрати даље сајбер нападе. Остаје да се види да ли ће окривљени затражити заштиту својих права пред Судом правде ЕУ, али је по нама тешко да до тога може да дође. Уосталом, поставља се питање колико рестриктивне мере у овом случају могу да буду делотворне, односно да довољно снажно казне учиниоце и спрече их да у будућности наставе са истим активностима. Делотворност санкција је увек отворено питање о коме би требало расправљати и у контексту рестриктивних мера ЕУ у сајбер простору, те се надамо да ћемо у неком даљем истраживању дотаћи и ту тему.

ЛИТЕРАТУРА

Вучић Михајло, „Брегзит – Преговори и могући исходи", *Дипломатија и безбедност*, Год I, Vol. 2, 2018, стр. 161-180.

Cardwell Paul James, "The Legalisation of European Union Foreign Policy and the Use of Sanctions", *Cambridge Yearbook of European Legal Studies*, Vol. 17, 2015, pp. 287-310.

Centre for European Policy Studies (CEPS), *Strengthening the EU's Cyber Defence Capabilities*, Brussels, 2018.

Council of the EU, Basic Principles on the Use of Restrictive Measures (Sanctions), 10198/1/04 REV 1, Brussels, 7 June 2004.

Council of the EU, "Restrictive measures (Sanctions): Update of the EU Best Practices for the effective implementation of restrictive measures", 8519/18, Brussels, 4 May 2018.

Council of the EU, Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ST/9564/2020/INIT, OJ L 246, 30.7.2020.

Council of the EU, Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), Brussels, 7 June 2017, 9916/17.

Council of the EU, Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, Brussels, 9 October 2017, 13007/17.

Council of the EU, Regulation 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ST/7302/2019/INIT, OJ L 129I, 17.5.2019, pp. 1–12.

Council of the EU, Decision (CFSP) 2018/1544 of 15 October 2018 concerning restrictive measures against the proliferation and use of chemical weapons, OJ L259/25.

Council of the EU, "Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy", 5664/2018, Brussels, 4 May 2018.

De Vries Anthonius W., Hadewych Hazelzet, "The EU as a New actor on the sanctions scene", International sanctions: between words and wars in the global system, eds. Peter Wallensteen and Carina Staibano, *International sanctions: between words and wars in the global system*, London, Frank Cass, 2005, pp. 95–107; Clara Portela, *European Union sanctions and foreign policy: when and why do they work?* Milton

Park: Routledge, 2010.

Eckes Christina, "Judicial review of European anti-terrorism measures—The Yusuf and Kadi judgments of the court of first instance", European law journal, Vol. 14, No. 1, 2008, pp. 74–92.

Eriksson Mikael, *Targeting peace: understanding UN and EU targeted sanctions*, Farnham, Ashgate, 2011; Giumelli Francesco, *The success of sanctions: lessons learned from the EU experience*, Farnham, Ashgate, 2013; Joakim Kreutz, "Human rights, geostrategy, and EU foreign policy 1989–2008", *International organization*, Vol. 69, No. 1, 2015, pp. 195–217.

EU, 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, *Official Journal of the European Union*, L218/8.

General Court of the EU, *Il Su-Kim & KNIC*, Judgment of the General Court (Third Chamber), 14 March 2018, ECLI:EU:T:2018:13.

Giumelli Francesco, Fabian Hoffmann, Anna Książczaková, "The when, what, where and why of European Union sanctions", *European Security*, 2020. DOI: 10.1080 /09662839.2020.1797685.

Giumelli Francesco, *How EU sanctions work: a new narrative*, Paris, EU Institute for Security Studies, 2013.

Kovačević Damir, Branko Krga, „Osnovni elementi Zakona o međunarodnim restriktivnim merama", *Vojno delo*, br. 3, 2015, str. 155-177.

Maass, Anna-Sophie *EU-Russia Relations, 1999–2015: From courtship to confrontation*, Routledge, London, 2016.

Miadzvetskaya Yuliya, "Challenges of the Cyber Sanctions Regime under the Common Foreign and Security Policy", *Security and Law*, eds. Anton Vedder, Jessica Schroers, Charlotte Ducuing, Peggy Valcke, KU Leuven Centre for IT & IP Law Series, Volume 7, 2019, pp. 277-297.

Missiroli Antonio, "The Dark Side of the Web: Cyber as a Threat", *European Foreign Affairs Review*, Vol. 24, Issue 2, 2019, pp. 135-152.

Novak Stjepan, „Uvodno o sankcijama Evropske Unije", *Zagrebačka pravna revija*, Vol. 2, No. 1, 2013, str. 61-73.

Rakić Branko M., „Evropski sud pravde između ljudskih prava i borbe protiv terorizma - odnos međunarodnog i evropskog prava", *Anali Pravnog fakulteta u Beogradu*, Vol. 57, Br. 2, 2009, str. 155-185.

Risse-Kappen, Thomas "Exploring the nature of the beast: international relations theory and comparative policy analysis meet the European Union", *Journal of common market studies*, Vol. 34, No. 1, 1996, pp. 53–80.

Sud pravde EU, Cases C-402/05 P and C-415/05 P, Presuda Velikog veća od 3. septembra 2008, ECLI:EU:C:2008:461.

Sud pravde EU, Cases C-584/10 P, C-593/10 P and C-595/10 P, Judgment of the Court (Grand Chamber), 18 July 2013, ECLI:EU:C:2013:518.

Tostensen Arne, Beate Bull, "Are Smart Sanctions Feasible?", *World Politics*, Vol. 54, 2002, p. 375.

Vučić Mihajlo, "European Union integration and the Belt and Road Initiative: A Curious case of Serbia", *Međunarodni problemi*, Vol. LXXII, No. 2, 2020, str. 337-355.

Mihajlo Vučić[62]

CHALLENGES OF THE APPLICATION OF RESTRICTIVE MEASURES OF THE EUROPEAN UNION AGAINST CYBER ATTACKS

Abstract

The paper deals with the topic of restrictive measures as an instrument of the common foreign and security policy of the EU, with special reference to restrictive measures against cyber attacks. The nature of the regime of restrictive measures, institutional and procedural decision-making mechanisms are emphasized, and then the focus of the analysis shifts to the specifics of restrictive measures against cyber attacks. The crucial role that the decision of the EU Council of Ministers of July 30, 2020 has for the further development of this area is emphasized, considering that for the first time in practice restrictive measures were applied against cyber attacks, specifically against persons belonging to the state structures of China, Russia and North Korea. The paper analyzes some obstacles to the practical application of restrictive measures, such as the protection of the rights of affected persons, the attribution of responsibilities and the harmonization of decisions between member states. The author concludes that in this area there is a gradual progress in the cooperation of member states and that in the future we can expect frequent use of restrictive measures as means of influencing the states that are behind cyber attacks.

Keywords: restrictive measures, sanctions, cyberattacks, EU, Council of the EU, common foreign and security policy.

62 Prof. dr Mihajlo Vučić, Research associate at the Institute of International Politics and Economics, e-mail: mihajlovucic@gmail.com