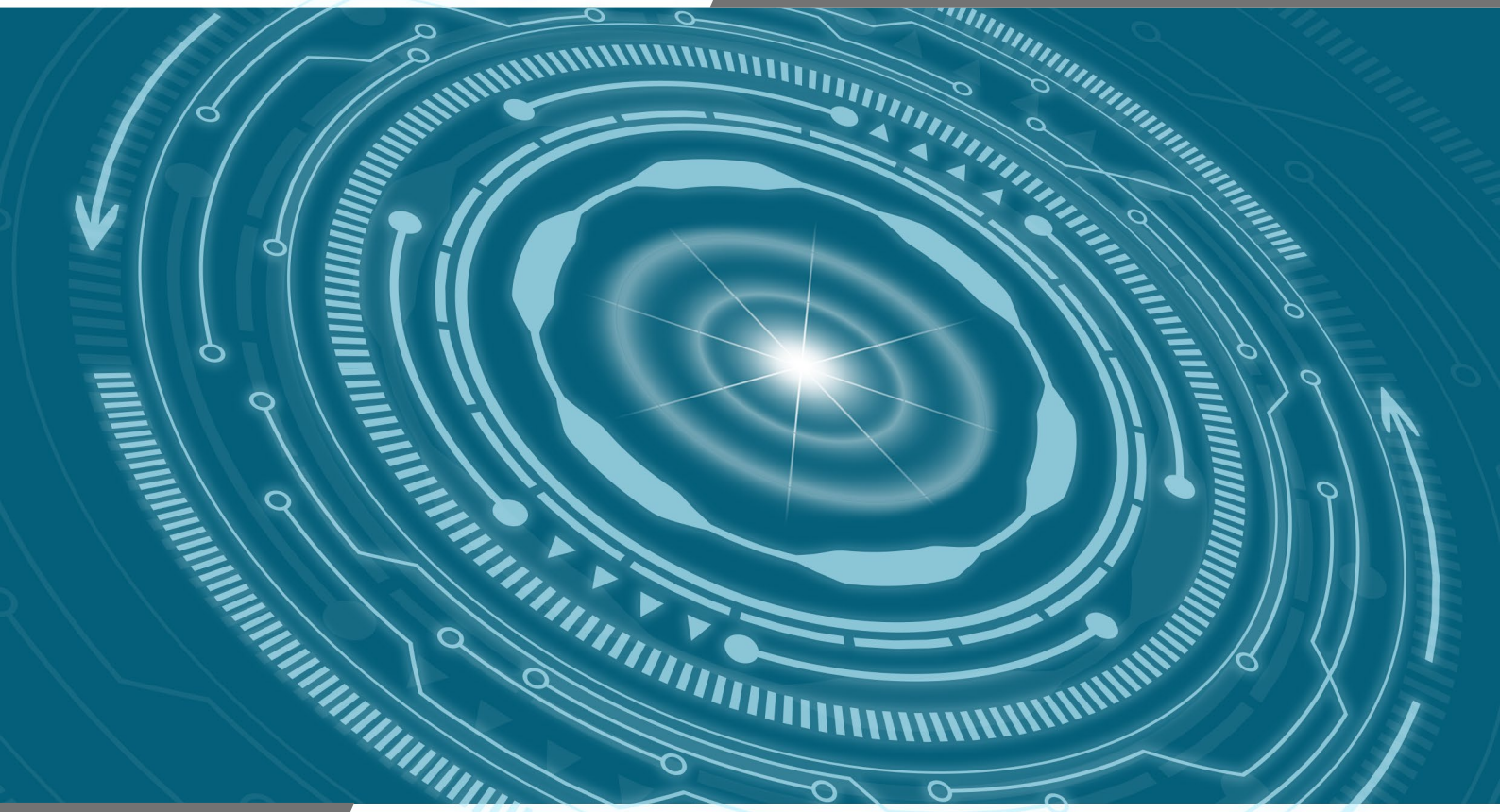
Ekonomi ve Dış Politika Araştırmalar Merkezi

edam

Siber Politikalar ve Dijital Demokrasi 2017/4



Aralık 2017

Hayaletlerin İzlerini Sürmek: Uluslararası Nitelikteki Siber Saldırıların Soruşturulması

Dr. Can Kasapoğlu | EDAM Savunma Analisti

Robert Bosch Stiftung
tarafından desteklenmiştir.

Hayaletlerin İzlerini Sürmek: Uluslararası Nitelikteki Siber Saldırıların Soruşturulması

Dr. Can Kasapoğlu

Siber saldırılar, uluslararası hukuk ve özellikle de silahlı çatışmalar hukuku çerçevesinde savaş eşiği altında kalan ancak barış dönemi devletler arası rekabet parametrelerinin de üzerinde seyreden hibrit bir konsept haline gelmekte ve aynı zamanda espiyonaj maksatları için de kullanılmaktadır. Dolayısıyla, birçok durumda, siber saldırıların ardında devlet düzeyindeki aktörler bulunsa da, 'vekil' unsurlar kullanarak kendilerini yoğun bir sis perdesi ardına gizlemektedirler. Açıkçası, gelişen teknoloji de bu tip yöntemlere daha büyük işlevsellik kazandırmaktadır.

Yönetici Özeti

Siber saldırılar, uluslararası hukuk ve özellikle de silahlı çatışmalar hukuku çerçevesinde savaş eşiği altında kalan ancak barış dönemi devletler arası rekabet parametrelerinin de üzerinde seyreden hibrit bir konsept haline gelmekte ve aynı zamanda espiyonaj maksatları için de kullanılmaktadır. Dolayısıyla, bir çok durumda, siber saldırıların ardında devlet düzeyindeki aktörler bulunsa da, 'vekil' unsurlar kullanarak kendilerini yoğun bir sis perdesi ardına gizlemektedirler. Açıkçası, gelişen teknoloji de bu tip yöntemlere daha büyük işlevsellik kazandırmaktadır.

Bir siber saldırı karşısında, istenilen düzey ve isabet oranıyla tespit yapılabilmesi için gerekli kanıt miktarı ve niteliği bir çok devlete hatta aynı devletin içindeki farklı kurumlara göre değişebilmektedir. Burada iyi anlaşılması gereken konu, teknik tespit ile söz konusu tespitin siyasi olarak deklere edilmesi arasında ciddi bir fark olduğudur. Özellikle başka bir devleti bir siber saldırıdan sorumlu tutmak düşünüldüğünden daha komplike bir olaydır. Hatta, saldırgan devlete böyle bir sorumluluk yükledikten sonra diplomatik retorik ötesine geçen bir adım atılmaması halinde, saldırıya uğrayan devletin caydırıcılık kapasitesinin zarar görmesi dahi olasıdır.

Yine yukarıda çizilen çerçeve ile ilintili olarak, bir siber saldırıdan sonra izlerin bizzat saldırgana mı, bilgisayara mı, saldırının arkasında olduğundan şüphe edilen devlete ya da devletlere mi doğru sürülmesi gerektiği halen kesin yanıtı verilmemiş bir sorudur. Daha açık ifade etmek gerekirse, bir siber saldırıyı gerçekleştiren bilgisayar ya da kişi tespit edildiğinde, söz konusu siber saldırıya ilişkin soruşturma tamamlanmış olur mu? Bu sorunun yanıtını teknik, siyasi, uluslararası hukuki mülahazalarla vermek mümkün olduğu gibi, stratejik istihbarat ve jeopolitik düzlemlerinde de bahse konu soruyu cevaplandırmak mümkündür. Burada kritik olan husus, her bir bakış açısının bizi farklı hedefe götüreceği gerçeğidir. Özellikle günümüzde revaçta olan çok-katmanlı siber saldırılar sonrasında istihbarat hedeflerinin ve soruşturmanın istikametinin ne olması gerektiği üzerinde ciddiyetle durulmalıdır.

Bir siber saldırı tespit edildikten ve hatta yeterince kanıt ışığında sorumluluk isnat edildikten sonra ne yapılacağı, yani bir siber saldırıya nasıl mukabele edileceği de büyük önem taşımaktadır. Zira, gelişen teknoloji ile siber saldırıların kinetik etki oluşturma kapasiteleri artmaktadır. Ayrıca, bir çok gelişmiş ülkenin kritik ulusal altyapılarının giderek daha çok dijitalize olması da ciddi tehditleri beraberinde getirmektedir. Bu konuda kimi yaklaşımlar aktif siber savunma konseptlerini ön plana çıkarmakta, önleyici ve ön alıcı yetenekler ile siber karşı saldırıları meşru görmektedir. İlk bakışta mantıklı görünse de, tespit aşamasında yaşanabilecek karışıklıklar aktif siber savunma yöntemlerinin daha büyük bir krize sebebiyet vermesini de beraberinde getirebilir. Hatta kimi istihbarat servisleri özellikle böyle bir provokasyonu hedefleyebilir.

Ayrıca, aktif siber savunma yetenekleri hayata geçirilse dahi, bir siber saldırıya mukabele ederken neyin meşru hedef teşkil edeceği tartışmalıdır. Bu noktada en ciddi sorun, siber alanı denetleyecek ve düzenleyecek uluslararası hukuki bir mekanizmanın ve kurumun bulunmamasıdır.

GİRİŞ

Siber saldırılar özellikle son dönemde gündemi sıklıkla işgal etmektedir. Konunun teknik mülahazaları kadar, uluslararası mahiyeti olan bir siber saldırının nasıl soruşturulması gerektiği de büyük önem taşımaktadır. Zira, savaş eşiği altında kalan siber çatışmalar aynı zamanda bir hibrit ve vekaleten mücadele konsepti haline gelmiştir. Benzer şekilde, siber yöntemler espiyonaj faaliyetlerinin de önemli bir parçasını teşkil etmektedir.

Bu çalışma, uluslararası ilişkiler düzleminde siber saldırıların tespiti ve bahse konu siber saldırılara ilişkin sorumluluk isnat edilmesi üzerine bir tartışma olarak kaleme alınmıştır. Çalışmanın amacı, konuya ilgi duyan okuyucular için giriş derecesinde bir referans oluşturmak ve henüz gelişmekte olan bu alanda yeni yayınları teşvik etmektir.

Bu rapor, öncelikle siber saldırganın tespit edilmesi ve sorumluluk isnat edilmesi üzerine genel bir değerlendirme yapacak, daha sonra siber saldırganların tespit edilmesinde teknik ve siyasi mülâhazalar arasındaki farkı açıklayacaktır. Müteakip olarak siber saldırılara nasıl mukabele edilmesi gerektiği ile ilgili tartışmalara yer verilecek, ardından siber alanda meşru hedef belirlenmesine ilişkin çeşitli görüşler aktarılacaktır.

Daha sonra, çok-katmanlı siber saldırılar üzerinde durulacak ve özellikle bu saldırılar karşısında tespit ve sorumluluk isnat etme alanlarında yaşanan zorluklar aktarılacaktır. Son olarak, alıntılanan bir senaryo üzerinden siber-uzayda gerçekleştirilen bir saldırının soruşturulmasındaki uluslararası hukuki ve siyasi zorluklar-ki bu zorluklar teknik zorlukların dahi ötesine geçebilmektedir-aktarılacaktır. Rapor, sonuç bölümündeki genel değerlendirmeler ile son bulacaktır.

Siber Saldırganın Tespit Edilmesi ve Sorumluluk İsnatı

Siber-uzayda tespit / isnat (attribution) konularını tartışmadan önce, bir siber aktörün kimliğinin belirlenmesi hususunun dahi oldukça karmaşık olduğu not edilmelidir. Günümüzde IP spoofing ya da botnet gibi yöntemlerin kullanımıyla üst düzey olmayan siber saldırganlar dahi kendilerini gizleyebilmektedirler. Dahası, herhangi bir siber saldırıyı 'düzenleyen' bilgisayarı tespit etmek, siber saldırganı tespit etmek anlamına da gelmeyebilmektedir. Örneğin, 2007 yılında Estonya'ya yönelik Rusya ile ilişkilendirilen geniş çaplı siber saldırılar, teknik olarak, ABD, Peru, Mısır gibi ülkelerdeki bilgisayarlardan kaynaklanmıştır.[1]

> Siber saldırılar birçok kez hibrit harp girişimlerinin ve vekaleten savaşın (proxy war) bir parçası olarak, devletler ile görünür bağlantıları tartışmalı gruplar tarafından yapılabilmektedir.

Ayrıca, herhangi bir saldırı ya da siber espiyonaj faaliyeti sonrasında esas saldırganlar -örneğin bir hacker grubu- tespit edildiğinde dahi, istihbari verilerle saldırının arkasında olduğu düşünülen devleti veya devletleri siyasi olarak sorumlu tutmak her durumda kolay değildir. Evet, birçok ülkenin "üniformalı hackerları" vardır, zira ABD, İsrail, Çin Halk Cumhuriyeti gibi birçok devlet resmi olarak siber komutanlıklar ve birlikler teşkil etmişlerdir.[2] Öte yandan, siber saldırılar birçok kez hibrit harp girişimlerinin ve vekaleten savaşın (proxy war) bir parçası olarak, devletler ile görünür bağlantıları tartışmalı gruplar tarafından yapılabilmektedir. Örneğin Gürcistan'a karşı 2008 yılı siber saldırılarını-ki bu saldırılar konvansiyonel bir harekata da eşlik etmiştir-gerçekleştiren aktörlerden biri Russian Business Network (RBN) adlı bir siber suç şebekesidir.[3]

Güvenlik, savunma ve askeri konularda herhangi bir saldırının ya da saldırgan davranışın failleriyle, amaçlarıyla ve kapsamıyla birlikte tespit edilmesi yaşamsal önemdedir. Üstelik, bu tespit ve isnat (attribution) gereksinimi salt siber çerçeve ile de sınırlı değildir. Söz gelimi, Suriye iç savaşı sırasında kimyasal saldırılarla ilgili sorumluluk isnatı hususları hep gündemin ilk sırasında olagelmiştir. Benzer şekilde, 2014 yılında Ukrayna üzerinde bir hava savunma füzesi tarafından düşürülen Malezya Hava Yolları uçağına yapılan saldırıya ilişkin de ciddi bir fail / kaynak belirleme sorunu olduğu söylenebilir.[4] Siber-uzayda bir saldırının failinin, konsept ve amaçlarının belirlenmesi, diğer güvenlik ve savunma sahalarına göre daha zor bir mahiyettedir. Öncelikle, internet siber saldırıları izlemek üzere dizayn edilmiş bir ağ karakteristiğine sahip değildir. Yani siber-uzayın 'coğrafyası' herhangi bir saldırganın kendisini gizlemesine ciddi olanaklar sunmaktadır. Buna ek olarak, siber ortamda tespit yapılabilecek 'kanıtlar' son derece manipülatif olabilmektedir.[5]

Esasen, özellikle hibrit harp koşullarında ve uluslararası hukuki zeminde savaş eşiği altında kalan çatışma durumlarında, saldırgan tarafların yukarıda belirtilen siber ortamdaki kanıtların manipülatif niteliklerinden fazlasıyla yararlandığı görülmektedir. Bahse konu manipülasyon, bu çalışmanın üzerinde derinlikle duracağı üzere, vekaleten harp ve çok-katmanlı siber saldırılar maskeleri ile daha da güçlendirilmekte, dolayısıyla siber saldırılar sonrasında ciddi bir sis perdesinin oluşmasına neden olmaktadır. Öte yandan, konjonktürel koşullara bağlı olarak savaş eşiği altında kalan mücadelenin sürmesi de, bir yandan siber saldırıların siyasi mesaj vermek için kullanılmasını beraberinde getirmektedir.

Teknik olarak, siber alanda tespit ve ilişkilendirme kavramı, siber saldırgan(lar)ın kimliklerinin (identity), yerlerinin (location) ve aracılarının (intermediary) belirlenmesi anlamına gelmektedir. Yapılan çalışmalar sonucu henüz emekleme evresinde olan literatür ve siber saldırılardan öğrenilen dersler, birkaç temel noktayı işaret etmektedir. Öncelikle, bir siber saldırı sonrası tespit / isnat çalışması, mevcut imkanlar dahilinde, gerçekten zordur. Özellikle, profesyonellik dereceleri

1 Bu konuda ayrıntılı bir değerlendirme için bkz. Marco, Roscini. World Wide Warfare – Jus ad bellum and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, Vol.14, 2010.

2 Ibid.

3 Ibid.

4 Thomas, Rid and Ben Buchanan. "Attributing Cyber Attacks", The Journal of Strategic Studies, Vol: 38, No: 1-2, 2015.

5 Ibid.

yüksek saldırganlar için birçok saklanma ve yanıltıcı yöntemlerden yararlanma imkanı vardır. Öte yandan, eğer saldırılan kurum içinde bir bağlantı var ise (insider) bugüne kadar edinilen tecrübeler soruşturmanın daha kesin sonuçlara ulaşma olasılığının yüksek olduğunu göstermektedir. Tespit / isnat (attribution) çalışmaları ile ilgili teknik düzeydeki önemli bir soru da, tespit edilen ya da edilmesi mümkün olan saldırgan ile ilgili ne yapılacağıdır. Bir yanıltıcı kullanılarak saldırganı tuzak bir hedefe çekmekten (honeypot), saldırgana 'işaretlenmiş' data göndererek kimliğini-aracı sistemler de dahil olmak üzere-iz sürerek bulmak (reverse flow) gibi birçok yöntem bulunmaktadır.[6] Ancak tüm bu yöntemlerin de belirli teknik gereksinimleri vardır. Örneğin bir honeypot, ancak yanıltıcı tuzağa yönelen siber saldırılar ile ilgili tespit yapabilir ve tuzağın bizatihi kendisinin incelenmesi dahi özel uzmanlaşma gerektirmektedir.[7]

Bu noktada, yukarıda aktarılan tespitlere ilişkin iki hususun vurgulanmasında yarar görülmektedir. Bunlardan birincisi, söz konusu aşamanın teknik bir zeminde tespit ve isnat ile sınırlı olmasıdır. Zira, işin içine siyasi sorumluluk isnat etme gerekliliği girince-bu çalışmada ayrıntılı olarak tartışılacağı üzere-durum teknik mülahazaların üzerine çıkmakta ve uluslararası ilişkilerin hassas dengelerine sıkı sıkıya bağlı olmaktadır. İkinci olarak, siber çatışmanın belki de en belirleyici parametresinin taarruzi tarafın savunma üzerinde doğal bir avantajının olmasıdır. Bahse konu avantaj, siber saldırı-siber savunma dengesi üzerinde de en ciddi belirleyen kimliğindedir. Bu nedenle, ileriki aşamalarda söz edileceği üzere, aktif siber savunma yaklaşımları da son dönemde giderek daha çok tartışılır hale gelmiştir.

Siber Saldırılarda Doğrudan ve Dolaylı İsnat

Siber saldırıların analiz edilmesi ve ilgili tespitlerin yapılmasında genel olarak iki temel kategoriden söz edilebilir. Bunlardan ilki saldırgan penetrasyonun tespiti (act attribution) ikincisi ise saldırganın bizatihi kendisinin tespitidir (actor attribution). Saldırgan faaliyet, esasen çok genel bir spektruma karşılık gelmektedir. Basit bir 'hack' girişiminden başlayarak, elektrik altyapısına, yani kritik ulusal altyapıya, yönelik stratejik ve kinetik etkileri olan saldırılar siber araçlar kullanılarak yapılabilir. Elbette, bu geniş spektrum karşısında, taarruza maruz bırakılan devletin de mukabele imkanları çeşitlidir. Söz konusu seçenekler firewall kapasitesinde artıştan, kapsamlı bir istihbarat çalışmasına, karşı siber saldırılardan kinetik mukabeleye kadar uzanmaktadır.[8]

Saldırganın ya da saldırganların tespit edilmesi ise daha karmaşık bir konudur. Dahası, ilk aşamada bulunan saldırganlar –söz gelimi saldırıyı gerçekleştiren bir hacker grubu– tespit edildikten sonra, söz konusu tespitin devlet düzeyinde bir aktöre uzanması ise çok kritik bir husustur. Bu nedenle, literatürde kategorik olarak, herhangi bir siber saldırı sonrasında bir devlete yönelik iki tip isnat durumundan bahsedilmektedir. Bunlardan ilki, doğrudan tespit ve isnat (direct attribution)[9] ikincisi de dolaylı tespit ve isnattır (indirect attribution). Doğrudan tespit durumunda, saldırganların bir devlet ile doğrudan bağlarının açıkça ortaya çıkarılmış olması gerekir. Dolaylı tespit durumunda ise, bir devlet doğrudan bir saldırı ile ilişkilendirilemese de, saldırıyı gerçekleştiren devlet-dışı grubun, kişi ya da kişilerin, söz konusu devlet ile daha gri alanlarda ilişkileri vardır.[10]

> Terörizmin etkili bir vekaleten harp yöntemi olmasının nedeni, devletlerin birçok durumda sorumluluklarını inkar edebilmeleri, terör örgütlerini desteklemenin konvansiyonel askeri harcamaların yanında çok düşük bir maliyetinin olması ve rakip devlete asimetrik yetenekler ile zarar verme kapasitesidir.

En nihayetinde siber saldırıların bir vekaleten savaş ve hibrit harp aracı olduğu unutulmamalıdır. Terörizmin etkili bir ve-

6 Attribution teknikleri ile ilgili bilgilendirici bir çalışma için bkz. David A. Wheeler and Gregory, N. Larsen, Techniques for Cyber Attack Attribution, Institute for Defense Analyses, 2003.

7 Ibid.

8 Eric F. Meija, "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework", Strategic Studies Quarterly, Spring 2014.

9 Ibid.

10 Ibid.

kaleten harp yöntemi olmasının nedeni, devletlerin birçok durumda sorumluluklarını inkar edebilmeleri, terör örgütlerini desteklemenin konvansiyonel askeri harcamaların yanında çok düşük bir maliyetinin olması ve rakip devlete asimetrik yetenekler ile zarar verme kapasitesidir. Siber saldırılar için tüm bu kriterlerin söz konusu olduğunu ve hatta terör eyleminin beraberinde getirdiği vahşet görüntülerinden kaçınılabildiği için kamuoyu tepkisini de aynı boyutta yükseltmediği bilinmelidir. Dolayısıyla siber saldırılar sonrasında birçok durumda doğrudan tespit ve isnat yapılması zordur. Diplomatik retorik düzeyinde suçlamalar gerçekleştirilse dahi, söz gelimi Estonya'ya 2007 yılında yapılan siber saldırılar sonrasında, Rusya Federasyonu'nu mahkum edecek yeterli etkinlikte bir kurum ya da norm henüz oluşturulmuş değildir. Bu nedenle, siber çatışma ortamında dolaylı tespit ve isnat durumlarının daha ağır bastığı söylenebilir.

Siber Saldırganların Tespitinde Siyasi Mülahazalar ve Aktif Siber Savunma Konseptleri

Siyasa üretimi ve siyasi-askeri siber strateji belirleme seviyesine gelindiğinde ise, karar vericilerin önünde daha ciddi tercihler bulunmaktadır. Bunlardan en dikkat çekici olanı da, henüz bir konsept olarak kaldığı görülen, aktif siber savunma (active cyber defense) kavramıdır. Özetle, aktif siber savunma bir siber saldırı gerçekleşmeden önceki (pre-emptive) aşamayı da kapsayacak şekilde, saldırgana misilleme seçeneklerini de içeren agresif bir savunma konseptidir. Bahse konu konseptin sunduğu çözümler kapsamında malware unsurlarını arayıp yok eden yazılımlardan (white worm) olası bir hackleme girişimine karşı taarruza (hack back) kadar uzanan geniş bir spektrum bulunmaktadır.[11]

Pasif bir siber savunma anlayışı, doğal olarak, var olan sistemlerin siber saldırılardan korunmasını önceler. Aktif siber savunma ise, siber saldırgana mukabele etmek amacıyla taarruzi önlemleri de beraberinde getirmelidir. Örneğin kimi uzmanlar, daha önce aktarılan honeypot uygulamalarının aktif bir siber savunma anlayışını yansıttığını değerlendirmektedir.[12] Benzer biçimde, botnet unsurlarını doğrudan hedef alan konseptler de bu kategoride tasnif edilirler. 2011 yılında FBI, ABD Adalet Bakanlığı ve (ISC) Internet Systems Consortium tarafından Coreflood botnet'e karşı yapılan siber taarruzi faaliyetler de aktif siber savunmaya örnek gösterilebilir.[13] Aktif siber savunma anlayışının bir örneği de 2012 yılında Gürcistan tarafından gerçekleştirilmiştir. 2011 yılından itibaren özellikle devlet e-sistemlerinde malware faaliyeti tespit eden Gürcü yetkililer, sistemlerini korumakla kalmamış, 2012 yılında saldırıyı gerçekleştiren Rusya'da üslenmiş bulunan hacker'ın bilgisayarına sızarak, kendi kamerası ile fotoğraflarını çektikten sonra söz konusu fotoğrafları uluslararası kamuoyuna da servis etmişlerdir.[14] Bu yöntem, doğrudan ve dolaylı sorumlu tutma anlayışlarının arasında bir yerde, daha yoğun ve somut bir propaganda çalışmasına örnek teşkil etmesi bakımından da önemlidir.

Aktif siber savunma ile ilgili bazı hukuki çekinceler bulunmaktadır. Öncelikle, bu konsept kapsamında kullanılan yöntemlerin bizatihi kendileri ofansif siber saldırılar anlamına gelebilmektedir. İkincisi, aktif siber savunmanın önleyici ve ön-alıcı saldırılara dayanması bahse konu çekinceleri daha ciddi bir hale getirmektedir. Ayrıca aktif siber savunma kapsamında, potansiyel siber saldırgana karşı önleyici vuruş tehdit altındaki ağ dışında bir sistemden de kaynaklanabilir. Bu da esasen bir siber saldırı demektir.[15] Bu nedenle NATO siber güvenlik çevreleri son dönemde aktif siber savunma anlayışının yerini 'Responsive Cyber Defense' (RCD) anlayışı ile ikame etmeye gayret göstermektedirler. Bu yaklaşım ile aktif siber savunma arasındaki temel fark, RCD'nin önleyici saldırı seçeneklerini portföyüne dahil etmemesidir. Yine de, söz konusu konsept kapsamında taarruzi imkanlar bir siber saldırıya verilebilecek meşru tepkilerin dışında tutulmamaktadır.[16]

Taarruzi seçeneklerin göz önünde bulundurulduğu hangi konsept tercih edilirse edilsin, kanımızca literatürde eksik bırakılan konu-özellikle hızla gelişen bilgisayar teknolojileri ile

[11] Robert, S. Dewar "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence", 6th International Conference on Cyber Conflict, NATO CCDCOE, 2014.

[12] Dorothy E. Denning ve Bradley J. Strawser, "Active Cyber Defense: Applying Air Defense to the Cyber Domain", Naval Postgraduate School, http://faculty.nps.edu/dedennin/publications/Active%20Cyber%20Defense%20-%20Cyber%20Analogies.pdf, Erişim tarihi: 14 Kasım, 2017.

[13] Ibid.

[14] Ibid.

[15] Robert, S. Dewar "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence", 6th International Conference on Cyber Conflict, NATO CCDCOE, 2014.

[16] Pascal, Brangetto, Tomas, Minarik ve Jan Stinissen, "From Active Cyber Defence to Responsive Cyber Defence: A Way for States to Defend Themselves – Legal Implications", NATO Legal Gazette.

> Siber saldırılar konjonktürel koşullardan bağımsız gelişmediği için, teknik düzeyi aşan siyasi isnatlar kapsamında stratejik istihbarat faaliyeti de önem arz etmektedir.

birlikte-içinde taarruzi yetenekleri barındıran herhangi bir savunma konseptinin sonuçlarının mutlaka siber alan ile sınırlı kalmayabileceğidir. Örneğin, İsrail Hava Kuvvetleri, Irak'ın nükleer programını akamete uğratmak için icra ettiği 1981 yılındaki harekat ile (Osirak Reaktörü'nün vurulması) 2000'li yıllarda İran'ın nükleer programını akamete uğratmak için icra ettiği Duqu ve Stuxnet kullanılan siber saldırılar, farklı yöntemler ile ancak benzer kinetik sonuçları oluşturmak üzere tasarlanmıştır. Ayrıca özleri itibariyle iki operasyon da önleyici bir nitelik taşımaktadır.[17] O halde, bir siber saldırıdan sonra tespit / isnat faaliyetlerinde isabetli yaklaşımlar her dönemde olduğundan daha büyük bir önem arz etmektedir ve gelecekte de bu önem artarak sürecektir. Zira siber yetenekler neden oldukları sonuçlar göz önünde bulundurulduğunda siber dünyanın sınırları dışına taşmaktadır.

Siber saldırılar konjonktürel koşullardan bağımsız gelişmediği için, teknik düzeyi aşan siyasi isnatlar kapsamında stratejik istihbarat faaliyeti de önem arz etmektedir. Daha önce vurgulandığı gibi, bir saldırının kaynağının ve niteliklerinin tespit edilmesi ve böylelikle söz konusu saldırıya ilişkin sorumluluk isnat edilmesi siber harp çerçevesinde kolay değildir. Özellikle saldırganın ve saldırının belirlenmesi, siber saldırıların doğası gereği zordur. Bir siber çatışma içinde, saldırıya maruz kalan aktör açısından yanıtlanması gereken iki soru vardır: saldırganın kimliği ve saldırganın nerede olduğu. 'Kim' ve 'nereden' sorularına ek olarak, bir de daha stratejik boyutta 'niçin' sorusunun sorulması ve yanıtının bulunması, özellike istihbarat fonksiyonları açısından büyük resmi tamamlar niteliktedir. Genelde, her siber saldırı öncelikle bir 'keşif' aşamasına dayanır. Bu aşamada, saldırgan hedefine ilişkin kritik bilgileri toplar. Keşif aşamasının olgunlaştığı aşamada bir siber saldırının tespit edilmesi ve saldırganın 'imzasının' belirlenmesi büyük önem arz etmektedir.[18] Elbette, bir siber saldırganın 'yeri' sanal ya da fiziksel olabilir. Ayrıca, siber saldırının kaynağının belirlenmesi siber saldırı ile saldırgan arasındaki köprülerin de (intermediary nodes) belirlenmesini gerektirmektedir. Zira, teknolojinin geldiği nokta itibariyle, siber saldırılar çok daha sofistike bir hal almıştır. Bu nedenle, modern belirleme yöntemlerinin en çok zorlandığı teknik engel, bir siber saldırının ilk kaynağının tespit edilebilmesidir.[19]

Siber saldırılar kapsamında, genel olarak, belirleme fonksiyonları yapısal bir zorlukla karşılaşmaktadır. Bu da, internetin esas olarak kullanıcının davranışlarını izlemek için değil, kullanıcılara ortak bir paylaşım platformu oluşturmak için dizayn edilmiş olmasından kaynaklanmaktadır. Ayrıca, siber saldırıları izleme bağlamında takip edilen yöntemler arasında, göndericinin / kaynağın kimliğinin değiştirilmesi önemli bir yer tutmaktadır. Zira, internet kullanıcılarının büyük çoğunluğu bilgi kaynağından ziyade içeriğiyle ilgilenmektedirler. Dahası, siber saldırıyı gerçekleştiren kaynağa ulaşmayı zorlaştıran birçok yöntem de bulunmaktadır.[20] Son olarak, siber saldırıların geldiği nokta itibariyle, gerçekleştirildikleri anda etki göstermeleri de gerekmez. Birçok siber ajan, belirli bir kuluçka süresinin ardından etkili olabilmektedir. Dolayısıyla, bir siber saldırının etkilerini gösterdiği an, siber saldırganın hedef ağa ya da sisteme sızdığı an olmak durumunda değildir.[21]

Siber Saldırılara Meşru Zeminde Karşılık Verilmesi: Tespit ve İsnat Aşamaları Sonrası

Bu noktaya kadar aktarılan siber saldırılara karşı tespit ve sorumluluk isnat edilmesine ilişkin tartışmaların ardından, en kritik konulardan biri de-belirli bir ölçüde-aydınlatılan bir siber saldırıya nasıl mukabele edileceğidir. Elbette, söz konusu mukabele konseptleri siber saldırının boyutları ve etkileri ile de orantılı olacaktır / olmalıdır. Söz gelimi, kritik ulusal altyapıyı geri dönülemez şekilde paralize eden bir siber saldırıya karşı verilecek yanıt ile göreli düşük seviyeli veri

[17] Tiong Pern, Wong. Active Cyber Defense: Enhancing National Cyber Defense, US Naval Postgraduate School, 2011, pp.26 – 27.

[18] Harsha K. Kalutarage, et.al. "Sensing for Suspicion at Scale: A Bayesian Approach for Cyber Conflict Attribution and Reasoning", 4th International Conference on Cyberr Conflict, CCDCOE, 2012.

[19] Rajesh Kumar, Goutam. "The Problem of Attribution in Cyber Security", International Journal of Computer Applications, Volume 131, No: 7, December 2015.

[20] Ibid.

[21] Ibid.

tabanlarına karşı düzenlenen bir siber espiyonaj faaliyetine verilecek yanıt, orantılılık prensibi dahilinde, aynı olmayacaktır. Her siber mütecaviz faaliyet karşısında mütekabiliyet esasına uygun bir yanıt verilmeyebilir. Örneğin, bu raporun yayıma hazırlandığı sırada, Birleşik Krallık Başbakanı Theresa May, Rusya Federasyonunu siber espiyonaj faaliyetleri ile suçlamış;[22] İspanyol Savunma Bakanı da yine Rusya Federasyonu ve Venezüela ile ilişkisi olan siber grupların Katalonya referandumu sürecine müdahil olduğunu ifade etmiştir.[23] Tüm bu iddialara karşın gerek Birleşik Krallık gerek İspanya Rusya Federasyonu ile barış dönemi koşullarını aşan bir kriz yaşamamıştır. Öte yandan, siber saldırılara ya da saldırı girişimlerine verilen tepkilerin diplomatik retorikten ya da karşı siber hamlelerden ibaret olduğu da düşünülmemelidir. Nitekim, yine bu yayının kaleme alınması sırasında, NATO ve AB üyesi Baltık devleti Estonya, bir Rus vatandaşını istihbarat servisi FSB ile ilişkili olmak ve siber saldırı hazırlığında olmak gerekçeleri ile tutuklamıştır.[24]

Siber-uzay, uluslararası hukuk kurallarının tamamen dışında bir alan olarak algılanmamalıdır. Bu konudaki görüşler, 'en azından' temel olarak, Birleşmiş Milletler (BM) Şartı'ndaki (2/4) tüm üye devletlerin uluslararası ilişkilerinde diğer devletler üzerinde güç kullanımı ve güç kullanımı tehdidinden kaçınacağına ilişkin taahhüdün siber alanı da kapsayacağını ortaya koymaktadır. BM Şartı çerçevesinde, güç kullanımının iki istisnası bulunmaktadır. Bunlardan ilki, Birleşmiş Milletler Güvenlik Konseyi (BMGK) tarafından güç kullanımının onaylanması kapsamındaki 42. Madde, diğeri de meşru müdafaa hakkını düzenleyen 51. Madde'dir.[25] Elbette, söz konusu iki uluslararası hukuki çerçeve de devletlere ilişkin mülahazalar içermektedir ve devlet dışı aktörlerin eylemlerini kapsamaz. Bununla birlikte, bir devlet, başka bir devletin (vekaleten) kullandığı devlet-dışı aktörün neden olduğu tehdide karşı meşru müdafaa hakkını kullanabilir. Ayrıca, eğer bir devlet-dışı örgütün yerleşip teşkilatlandığı 3. Ülke (host nation) bahse konu devlet-dışı saldırgan grubu bertaraf etmiyor ya da edemiyor ise, bu devlet-dışı aktörden zarar gören mağdur durumundaki devlet, egemenliği altındaki ülkeyi korumak için saldırgan devlet-dışı aktörün faaliyetlerini güç kullanarak engellemeyi tercih edebilir.[26]

Yukarıda aktarılan uluslararası ilişkilerde güç kullanımına ilişkin tüm tasarruflar, silahlı çatışmalar hukuku (the law of armed conflicts-LOAC) çerçevesinde yapılmak durumundadır. Dolayısıyla, gerek teorik gerek uygulama bağlamında, günümüz güvenlik bilimleri literatürünün en önemli tartışma konularından biri de silahlı çatışmalar hukuku ile uluslararası hukuktaki güç kullanımı ve meşru müdafaaya ilişkin hususların siber-uzayda hangi kapsamda geçerli olacağı ile ilgilidir. Bu çerçevede bir başka önemli husus da siber-uzayda ve siber çatışma içinde hedef tespiti ile ilgilidir. Zira, birçok 'siber araç' ya da 'siber ajan' hem sivil hem de askeri amaçlar için yararlanılan, çift kullanımlı (dual-use) bir niteliğe sahip olabilir. Bu konuda literatürde sıklıkla yararlanılan analoji 'köprü'dür. Tamamen sivil mimari amaçlarla inşa edilmiş bir köprü, askeri harekat sırasında birliklerin ve platformların intikali için çok kritik bir avantajı beraberinde getirebilir.[27] Dahası, çift-kullanımlı bir niteliğe sahip olmasına rağmen, harp ortamı için stratejik olan bir köprünün hedef alınması (elbette bölgede sivillerin varlığı gibi parametreler de dikkate alınarak) birçok durumda silahlı çatışmalar hukuku bağlamında meşru hedef teşkil edebilmektedir. Silahlı çatışmalar hukuku kapsamında bir 'objenin' meşru hedef olabilmesi için, doğası, nitelikleri, konumu ve kullanım amacı itibariyle ayırıcı biçimde askeri bir katkı yapması; ayrıca, kısmi ya da tam olarak bertaraf edilmesi durumunda ciddi düzeyde askeri avantaj oluşturması gerekmektedir. Bir siber saldırıya, siber aktöre ya da siber ajana silahlı çatışmalar hukuku kapsamında yanıt verilmesi için yukarıda belirtilen iki kriterin karşılanması zaruridir. Yine de, tüm şartların yerine getirildiği bir durumda dahi, ikincil hasar (collateral damage) olasılığının dikkate alınması gerekmektedir.[28]

Dolayısıyla bir siber saldırı karşısında askeri yanıt verilmesi, popüler kimi yorumlarda dile getirildiğinin aksine, kategorik bir konsept olarak düşünülmemelidir. Tıpkı siber saldırılara ve siber savunma imkanlarına ilişkin teknolojik gelişmeler

22 Guardian, https://www.theguardian.com/politics/2017/nov/13/theresa-may-accuses-russia-of-interfering-in-elections-and-fake-news?CMP=Share_iOSApp_Other, Erişim tarihi: 17 Kasım 2017.

23 El Pais, https://elpais.com/elpais/2017/11/10/inenglish/1510329788_994258.html, Erişim tarihi: 17 Kasım 2017.

24 Reuters, https://www.reuters.com/article/us-estonia-russia-fsb/estonia-arrests-suspected-russian-fsb-agent-idUSKBN1D71I0, Erişim tarihi: 17 Kasım, 2017.

25 Eric, F. Mejia, "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework", Strategic Studies Quarterly, Spring 2014.

26 Ibid.

27 Ibid.

28 Ibid.

gibi, bu alandaki uluslararası hukuk normları da-teknolojik gelişmelerin arkasından gelse de-gelişme göstermektedir. Bununla birlikte, pratik ile hukuki anlayış arasındaki makasın açık olmasının en önemli nedenlerinden belki de birincisi, siber alanı düzenleyecek uluslararası meşruiyet sağlayıcı bir kurumun bulunmaması ve normların da henüz gündeme geliyor olmasıdır.

Elbette, 'siber saldırı' kavramının tanımlanması da, siber saldırılarda tespit ve isnat problemlerinin belirlenmesi açısından kritik önem taşımaktadır. Özellikle bir siber enstrüman ile icra edilen eylemin hangi durumlarda silahlı saldırı ya da güç kullanma kategorilerine girdiğinin tespit edilmesi uluslararası ilişkiler çerçevesinde dikkatle tetkik edilmesi gereken bir konudur. Birçok durumda, özellikle de gelişen teknoloji ile birlikte, siber saldırılar kinetik etkiler oluşturabilir. Bununla birlikte, siber saldırıları güç kullanımı kategorisinde değerlendirsek dahi, karşımıza daha önemli bir sorun çıkmaktadır, "kimin sorumlu tutulması gerekecektir?". Bu nedenle, silahlı çatışmalar hukukunun uygulanmasını savunan uzmanlar dahi, 'siber savaş' kavramının konvansiyonel savaş parametrelerinden çok farklı olduğunu kabul etmektedirler. Konvansiyonel harp, birçok durumda muharip tarafların açık ve belirgin oldukları bir silahlı çatışma niteliği gösterir. Bir siber saldırı ise yalnızca saldırının teknik detaylarını değil, aynı zamanda saldırganı ya da yönlendirenleri de gizleme amacı gütmektedir.[29] Ünlü Stuxnet vakasında gözlemlendiği gibi, siber saldırılarda kullanılan 'mühimmat-yani malware-görevini icra ettikten sonra kendisini de yok etmek üzere programlanabilir. Ayrıca, yine bu 'siber ajanlar ' çok spesifik bir alanda görev yapmak üzere tasarlanabilirler. Nitekim, Stuxnet yalnızca santrifüj kontrol mekanizmasına zarar vermek üzere programlanmıştır. Ayrıca, siber saldırılarda 'atış vasıtası' yetenekleri de saldırganın kimliğine ulaşmayı çok karmaşık hale getirmektedir. Gürcistan'a yönelik 2008 yılında gerçekleştirilen DDoS siber saldırıları bu duruma örnek teşkil etmektedir.[30]

Öte yandan, bu noktada her siber penetrasyonun siber saldırı olarak tanımlanamayacağı da not edilmelidir. Siber espiyonaj faaliyetlerini saldırı olarak değerlendirmek mümkün değildir. Örneğin bu raporda örnek verilen Rusya kaynaklı Birleşik Krallık ve İspanya üzerindeki dezenformasyon, manipülasyon ve siber-espiyonaj konuları, birer siyasi krizin parçaları olsa da, uluslararası hukukta güç kullanımı kategorisinde değerlendirilmemelidir. Bununla birlikte, siber saldırıların da çoğu kez siber espiyonaj faaliyetleri sonrası vuku buldukları unutulmamalıdır.[31]

Gelinen nokta itibariyle siber saldırılarda tespit ve isnat sorunlarına ilişkin genel bir anlayış teşkil ettikten sonra, daha kompleks siber saldırı profillerine geçilebilir. Literatürde son dönemde kavramlaştırılan çok-katmanlı siber saldırılar, bir mütecaviz girişimden 'kimin sorumlu tutulması gerektiği' sorusunu çok boyutlu bir düzleme taşımaktadır.

Çok-Katmanlı Siber Saldırılarda Sorumluluk İsnatı ve Karmaşık Uluslararası Hukuki Zemin

Siber saldırıların ve siber espiyonaj girişimlerinin soruşturulması aşamasında, çok katmanlı (multi-stage) saldırılar oldukça çetin vakalar olarak ön plana çıkmaktadır. Bir bilgisayarın zincirleme olarak diğer bilgisayarları ele geçirerek saldırı düzenlemesi anlamına gelen söz konusu ardışık penetrasyonlar, teknik, hukuki ve siyasi komplikasyonları da beraberinde getirmektedir. Dolayısıyla çok katmanlı siber saldırılara dikkat çeken uzmanlar, mevcut ağ yapısı daha etkin tespit amacıyla modifiye edilse dahi, giderek yaygınlaşan çok katmanlı saldırıların siber güvenliğin karmaşık problem alanının daralmasına izin vermeyeceği görüşündedirler. Ayrıca, mevcut telekomünikasyon yapısının tespit sorunlarına yönelik teknik değişimler geçirmesi ihtimali insan hakları, kişisel verilerin korunması ve benzer konularda endişeleri de beraberinde getirmektedir.[32] Dolayısıyla özgürlük-güvenlik dengesinin siber alanda da mevcut olduğu bir gerçektir. Nitekim siber alanın düzenlenmesine ilişkin BM zemininde getirilen öneriler çerçevesinde, Rusya Federasyonu, Çin Halk Cumhuriyeti gibi aktörlerin kısıtlayıcı yaklaşımları genel paketlerin içinde takdim etmeleri de endişe edilen bir husustur.

Çok katmanlı gerçekleşebilecek bir diğer saldırı türü de, kritik ulusal güvenlik bilgilerinin sistemdeki açıkların kullanılma-

[29] Bu konuda detaylı bir çalışma için bkz. Wylie, McDade. Attribution Delayed Attribution and Covert Cyber – Attack: Under What Conditions should the United States Publicly Acknowledge Responsibility for Cyber Operations, US Naval Postgraduate School, Monterey California, 2014.

[30] Ibid.

[31] Ibid.

[32] David D. Clark ve Susan Landau, "The Problem is not Attribution; It's Multi – Stage Attacks", 2010, http://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/11-Clark.pdf, Erişim tarihi: 08 Kasım 2017.

sı yoluyla sızdırılmasıdır.[33] Daha önce Amerika Birleşik Devletleri'ne yönelik Kuzey Kore (2009) ve Çin (2014) kaynaklı olduğu düşünülen bu kategorideki saldırılarda da, zincirleme olarak penetre edilmiş ve farklı lokasyonlarda bulunan araçlar kullanılmıştır.[34] Dolayısıyla siber-uzayda yaşanan rekabet ve çatışma, uluslararası ilişkilerin diğer ajandalarından ayrı düşünülmemelidir. Bu nedenle, teknik tespit / isnat (attribution) için gerekli olan kanıtlar ve bu kanıtlara ilişkin eşik, bir devletin teknik zemindeki bulgularını siyasi zemine taşıması için her durumda yeterli olmayabilir. Siber saldırılar, hem teknik düzeyleri hem de hedefleri (siyasi, ideolojik, ekonomik, vb.) bağlamında değişkenlik gösterirler. Saldırının teknik beceri düzeyi arttıkça, saldırganı bulmak da aynı oranda güçleşmektedir. Ayrıca, teknik imkanlar neticesinde ilk saldırganın kimliğine ulaşmak, günümüz dünyasında siyasal tepki vermek için yeterli değildir.[35]

Dolayısıyla Anglo-Amerikan siber güvenlik literatüründe 'attribution' olarak geçen konsept, her durumda aynı anlamı ifade etmeyebilir. Özellikle çok-katmanlı saldırılar failin tespitini çok karmaşık bir hale getirmektedir. Herbert Lin, Hoover Institution için kaleme aldığı çalışmasında bu durumu ilginç bir örnekle açıklamaktadır. Lin, San Fransisco'da bulunan bir Savunma Bakanlığı bilgisayar sisteminin –sistemden Tony adında hayali bir karakterin sorumlu olduğu belirtilmiştir– bir saldırıya maruz kaldığını farz etmektedir. Sisteme giriş yetkisi olmayan biri -Lin'in senaryosuna göre 'George'-, siber yöntemler ile bilgisayar ağının kontrolünü ele almıştır. Yapılan ilk araştırmadan sonra, saldırıya neden olan aktivitelerin kaynağı olarak, Arkansas çevresinde yaşayan 84 yaşında bir kadının bilgisayarı tespit edilmiştir. Öte yandan bahse konu bu bilgisayar, Yunanistan'da bulunan başka bir bilgisayar tarafından ele geçirilmiştir. Bu bilgisayarı kullanan kişi hayali George karakteridir, bahse konu saldırıyı Yunanistan'dan bir bilgisayar ile gerçekleştirmiştir.[36] Hikayeyi daha ilginç hale getiren ise, George'un vatandaşlık ve organizasyon bilgileri olarak karşımıza çıkmaktadır. George, Çin Halk Cumhuriyeti pasaportu taşımaktadır, bununla birlikte bilinen bir Rus hacker grubunun da üyesidir. Bu Rus hacker grubunun lideri, hikayeye göre Sergey, Rus Federal Güvenlik birimi FSB Başkanı ile yakın arkadaştır. Yapılan istihbarat çalışmaları, George'un üyesi olduğu Rus hacker grubu lideri Sergey adlı hayali karakterin, yaklaşık iki hafta önce FSB Başkanı ile yemek yediğini ve raporlara göre yemekte konuşulan konulardan birinin de San Fransisco'da bulunan ABD Savunma Bakanlığı tesisi olduğunu belirtmiştir.[37]

Lin, bu çok ilginç kurgusunda yukarıdaki senaryo bilgilerini de verdikten sonra, kritik 'attribution' sorunusu sormaktadır: San Fransisco'da yaşanan siber saldırıdan kim "sorumludur"? Burada karşımıza üç ana tespit / isnat / sorumluluk yükleme (attribution) konsepti ve bu üç konseptin de verdiği yanıtlar çıkacaktır:[38]

- İlk yaklaşım, saldırının izini kaynak makineye doğru sürmektir. Yukarıdaki örnekte saldırının izini makineye, yani bilgisayarlara ulaşmak için sürmek, soruşturmanın istikametini öncelikle Arkansas'da yaşayan 84 yaşındaki Amerikalı kadın karaktere çevirecektir. Buradan da, söz konusu hayali kadın karakterin IP adresi belirlenmiş olan bilgisayarına penetrasyon gerçekleştirmiş olan diğer bilgisayarlara, yani Yunanistan'da bulunan hayali George karakterinin kullandığı bilgisayarlara doğru ilerlenecektir. Dolayısıyla soruşturmada karşılaşılan tablo, birden çok bilgisayarın zincirleme kullanıldığı bir intrüzyon durumudur (multi-stage intrusion). Belirtilen konsept belirli düzeyde sonuç vermiştir, ancak soruşturmanın kapasitesi George karakterinin Yunanistan'daki bilgisayarlarına ulaştığı anda da tükenmiş ve çok katmanlı intrüzyon teşhisi ile dosya kapanmıştır. Elbette bu noktada önemli bir detay da bulunmaktadır. Girişimin son halkası olan hayali bilgisayar Arkansas'dadır. Eğer bahse konu bilgisayar başka bir ülkede olsa idi, bu durumda da güvenlik güçlerinin uluslararası işbirliği konusu gündeme gelecektir.[39]

- İkinci yaklaşım, saldırının izini insan unsurlarına doğru sürmek şeklinde karşımıza çıkmaktadır. Burada ilk

[33] Ibid.

[34] Defense One, http://www.defenseone.com/ideas/2017/09/winter-here-us-not-ready-cyber-war/140850/, Erişim tarihi: 08 Kasım 2017.

[35] Paul Cornish, et.al. On Cyber Warfare, Chatham House, London, 2010, p.20.

[36] Referans verilen dikkat çekici siber tespit / isnat (attribution) senaryosu için bkz. Herbert Lin. Attribution of Malicious Cyber Incidents, Hoover Institution, Aegis Paper Series No. 1607, 2016, pp.5–13.

[37] Ibid.

[38] Ibid.

[39] Ibid.

öncelik, saldırıyı kimin ya da kimlerin gerçekleştirdiğini tespit etmektir. İncelemeye konu hayali durumda, insan unsurunun izi sürüldüğünde hedef Yunanistan'daki bilgisayar değil, onu kullanan George karakteri olmalıdır. Ancak salt teknik siber imkanlar ile kimin saldırıdan sorumlu tutulan bilgisayarları kullandığını belirlemek mümkün görünmemektedir. Ayrıca, "bir arabanın kazaya karışmış olması, muhakkak arabanın sahibinin kaza yaptığını göstermediği gibi", bir bilgisayarın herhangi bir siber saldırıyla ilişkilendirilmesi de sahibinin ilişkilendirilmesi için yeterli kanıt sunmamaktadır. O halde, incelemeye konu senaryo kapsamında, saldırıyı bir ya da birkaç hacker grubu ile ilişkilendirecek 'dijital kanıtlar ve parmak izleri' aranması gerekmektedir. Ayrıca, George adlı hayali karakterin bağlantılı olduğu grup, kişi ve kurumlar için de ayrıca istihbarat çalışması gerçekleştirilmesi uygun olacaktır. Bu konsept kapsamında öncelikli amaç, şüphelenilen George karakterini ilgili saldırıdan sorumlu tutmaya yetecek kanıtlara ulaşmaktır. Elbette, buradaki 'yeterlilik kavramı' birçok devlet ve hatta kuruma göre değişiklik gösterecektir. Farklı durumlarda, birçok zayıf kanıtın bir kişiyi, grubu veya devleti işaret edebileceği gibi, az sayıda çok güçlü kanıtlar da aynı işlevi görebilir. İstihbarat soruşturmasının 'mümkün olduğu kadar çok kanıta mı', 'mümkün olduğu kadar güçlü kanıta mı' ulaşma önceliği taşıyacağı ise karar vericilerin tasarrufundadır. Şurası anlaşılmalıdır ki, siber dünyada 'kanıt' kavramı çok katmanlıdır.[40] Örneğin, internet servis sağlayıcısı –normal koşullarda–, bir epostanın kim tarafından hangi adrese gönderildiğini belirleyebilir. Ancak, –yine olağan koşullarda– eğer söz konusu epostaya iliştirilen bir içerik özel kriptolama işlemine maruz kalmış ise tespiti kolay olmayacaktır. Yine de gelişen teknoloji ve teknik yetenekler ile sadece hedef bilgisayarı değil, kullanıcı kişiyi de bulmaya yönelik yeni imkanların kullanılması mümkündür. Örneğin, hemen her insan, klavye kullanırken tuşlara farklı bir tempo ile basar. Mikro düzeyde analiz gerektiren bu ipucu, modern istihbarat araçlar ile artık izi sürülebilir bir nitelik kazanmıştır.[41] Yine de, bu ikinci konseptin de eksik kaldığı bir boşluk bulunmaktadır. Diyelim ki, siber güvenlik soruşturması hangi bilgisayarın bahse konu saldırıdan sorumlu olduğunu ve bu bilgisayarın da büyük ihtimalle George hayali kişisi tarafından kullanıldığını tespit etti, yine de söz konusu hayali hacker karakterine bu saldırıyı gerçekleştirme direktifini kimin verdiği hala yanıtlanmamış bir soru olacaktır.[42]

- İncelemeye konu hayali siber olayda fail olan George karakteri, kendi başına hareket etmiş olabileceği gibi, bu denli geniş çaplı bir siber saldırıda kimi zaman devletlerin de içinde olduğu sponsorlar ve yönlendiriciler bulunmaktadır. Dolayısıyla, üçüncü konsept, "kim yaptı" sorusu yerine, "kim suçlanmalı" sorusuyla ilgilenir. Teknik istihbarat araştırması ile George hayali karakterinin hangi grup ya da servis için çalıştığının belirlenmesi doğal olarak kolay değildir. Bununla birlikte diğer istihbarat verileri ile failin bağlantıları bulunabilse dahi, uluslararası hukuki çerçevedeki boşluklar ve tartışmalar isnat sahasındaki karmaşayı da beraberinde getirecektir. Örneğin, incelemeye konu senaryoda George karakteri Yunanistan'da bulunan bir Çin Halk Cumhuriyeti vatandaşıdır. O halde, Atina'nın veya Pekin'in suçlanması mümkün müdür? Ya da, George farazi kişisinin bir Rus hacker grubu ile ilişkisi göz önünde bulundurulduğunda, ve bu grubun liderinin FSB başkanı ile ilişkileri de düşünüldüğünde, bu grubu ya da Rusya Federasyonu'nu sorumlu tutmak ne kadar olasıdır? Kesin bir isnat için hangi zemin ve kanıtlar gerekmektedir?[43]

Açıkçası, günümüz devletler arası ilişkilerinde yukarıda aktarılan soruların yanıtlarını vermek teknik kanıtlardan çok siyasi mülahazalara dayanmaktadır.

Yine de bilinmesi gereken şudur. Yukarıda açıklanan üç siber tespit / isnat modeli de birbirleri ile bağlantılıdır ancak her durumda aralarında doğrudan bir ardışık ve sistematik ilişki bulunmayabilir. Söz gelimi, hangi bilgisayarların saldırıdan sorumlu olduğunu bulmak her durumda hangi kişilerin sorumlu olduğunu bulmak anlamına gelmeyeceği gibi, hangi kişilerin sorumlu olduğunu bulmak da birçok kez saldırının arkasında esasında hangi devlet ya da devlet-dışı grubun bulunduğunu tespit etmek anlamına gelmeyecektir. Bununla birlikte, pratikte bu üç yaklaşım bir arada çalışır.[44] Eğer

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Ibid.

zincir içindeki ilk bilgisayarların hangi ülkede bulundukları tespit edilebilir ise bu-normal şartlarda-faillerin söz konusu ülkedeki bilgisayarlara erişimi olduğu anlamına gelecektir. Eğer tespit edilen ülkede internet kullanıcıları ve hatta hacker grupları / kişileri sınırlı ise, bu durumda da üzerinde çalışılacak daha dar bir olağan şüpheliler listesine ulaşılacaktır. Daha sonra, bahse konu kişiler üzerinden siber saldırının yönlendiricilerinin ve sponsorlarının tespit edilmesine çalışılacaktır.[45]

Bazı uzmanlar, bir siber saldırının devlet düzeyinde herhangi bir aktör ile ilişkilendirilmesi için gerekli uluslararası hukuki zeminin teşkil edilmesinin bu tür saldırıların engellenmesi için zaruri olduğunu belirtmektedirler. Zira, savaş hukuku da örtülü saldırıları yasaklamaktadır.[46] Şurası kesindir ki, özellikle yukarıdaki örnekte görülen çok aşamalı siber saldırılara karşı, tespit / isnat & belirleme yeteneklerinin güçlü olması başlı başına bir caydırıcılık unsurudur. Yine de, siber alan dışında kalan uluslararası ilişkiler kapsamındaki olaylar için tespit kapasitesi, siber alana göre daha sonuç alıcıdır.[47] Dolayısıyla, en azından yakın dönemde, siber saldırı ve penetrasyonların cezalandırılacağı bir uluslararası hukuk mekanizmasının etkin biçimde işleyeceğini öngörmek mümkün görünmemektedir.

Siber-uzayda gerçekleşecek çatışmalarda doğru tespit yapmak kadar, tespit ve isnat sürecinin hızlı olması da büyük önem taşımaktadır. Bahse konu süratli tespit yeteneği, yalnızca savunma ile sorumlu kurum ve kişiler için değil, politik karar alıcılar için de bir zaruret niteliğindedir. 2010 yılında Birleşik Krallık düşünce kuruluşu Chatham House tarafından 'Siber Harp Üzerine' başlığıyla yayımlanan bir rapor, siber olaylara müdahale konusunda yeni nesil uzmanların -"digital natives"- bürokratik ve siyasi kadroları doldurdukça olayların daha hızlı akacağını değerlendirmektedir.[48] Söz konusu rapor, çarpıcı bir biçimde, siber saldırılara karşı statik bir savunma ve tespit mekanizması oluşturma denemelerini İkinci Dünya Savaşı sırasındaki Fransız Maginot Hattı'na benzetmektedir. Buna göre siber-uzayın kaotik ortamında statik bir savunma anlayışına yer yoktur, olmamalıdır.[49]

Siber savunma alanında literatürde genel kabul gören stratejik çerçeve, siber saldırıların önlenmesi, cezalandırılması ve uluslararası işbirliği olmak üzere üç ana kategoride fonksiyonlar oluşturmayı amaçlamaktadır. Bu yapının ilk ayağı olan siber saldırıların engellenmesi ve caydırılması, özellikle kritik ulusal altyapıların korunması ve bir devletin yönetim fonksiyonlarının aksamadan sürmesi açısından önem taşır. Telekomünikasyon ve bilişim sistemleri ile bilgisayar ağ altyapılarının siber saldırılara karşı güçlendirilerek daha dayanıklı hale getirilmesi caydırıcılığın bir parçası olarak kabul edilmektedir. Burada amaç, caydırıcılığın 'herhangi bir siber saldırının istenilen sonuçları veremeyeceği' algısını oluşturarak temellendirilmesidir. Böylelikle, gerek kritik ulusal altyapının gerekse bilgi sistemlerinin potansiyel saldırgan için 'çekici' olması engellenmeye çalışılır. Bu noktada, ülkeden ülkeye değişmekle birlikte, kritik ulusal altyapının bir bir bölümünün özel sektörün işletmesinde olması bahse konu caydırıcılık anlayışının kompleks parametrelere sahip olmasını beraberinde getirmektedir.[50]

İncelemeye konu stratejik çerçevenin ikinci ayağında, gerçekleştirilen bir siber saldırının failinin 'cezalandırılması' bulunmaktadır. Bu tür bir konsept doğal ofansif siber yeteneklere sahip olunmasını da beraberinde getirmektedir. Siber çatışma içinde herhangi bir siber saldırganlığın cezalandırılması için muhakkak askeri imkanların kullanılması gerekmemektedir.[51] Kaldı ki, daha önce bu rapor kapsamında vurgulandığı üzere, bir siber saldırıya alışılageldik askeri araçlar ile karşılık verilmesi uluslararası hukuktaki orantılılık ilkesi ile de-en azından mevcut kinetik etkiler bağlamında-bağdaşmayacaktır. Dolayısıyla 'klasik' bir siber saldırıya karşı yapılabilecekler arasında uluslararası yaptırım yoluna gidilmesi, siyasi adımlar ve-henüz inşa edilen-hukuki süreçlerin işletilmesi bulunmaktadır.

Yine de, orantılılık ilkesi içinde dahi, askeri yetenekler ile mukabele edilmesi gereken siber saldırılar-teorik olarak-orta ve

---

45 Ibid.

46 Scott, J. Shackelford, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem", C. Czosseck ve K. Podins [ed.], Conference on Cyber Conflict Proceedings 2010, CCDCOE, 2010, Tallinn.

47 David D. Clark ve Susan Landau, "The Problem is not Attribution; It's Multi – Stage Attacks", 2010, http://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/11-Clark.pdf, Erişim tarihi: 08 Kasım 2017.

48 Paul Cornish, et.al. On Cyber Warfare, Chatham House, London, 2010, p.20.

49 Ibid.

50 Antonia Chayes. "Rethinking Warfare: The Ambiguity of Cyber Attacks", Harvard National Security Journal, Vol.6, 2015.

51 Ibid.

uzun vadede vuku bulabilir. Kritik ulusal altyapıya ya da söz gelimi bir bir nükleer tesise yönelik güçlü siber saldırılar tıpkı bir hava bombardımanı gibi kinetik etkiler üreterek ölümlere ve yıkıma neden olabilir. Zaten bu ihtimaller nedeniyle, bir siber saldırının fail ya da faillerinin belirlenmesi önem arz etmektedir. Zira, bir yandan hızla gelişen teknoloji yukarıda sözü edilen çok yüksek yıkıcılıkta kinetik etki oluşturabilecek siber saldırılar icra etme imkanlarını gündeme getirirken, diğer yandan da kritik ulusal altyapılar giderek daha çok bilgisayar ağlarına bağımlı hale gelmektedir. Felaket düzeyinde yıkıcılığa sahip bir siber saldırı sonrasında faile ilişkin tespitin yanlış yapılması-veya gerçek failler tarafından yanlış tespite neden olacak yanıltıcılıkta izler bırakılması (false flag)-uluslararası bir krize neden olabilir.[52]

Önleme & caydırıcılık ve cezalandırma dışında, incelemeye konu stratejik çerçevenin üçüncü ayağını uluslararası işbirliği kapasitesi oluşturmaktadır. Özellikle 2007 yılında Estonya'yı hedef alan siber saldırılar sonrasında bu alanda uluslararası işbirliğinin önemi daha da belirginleşmiştir.[53] Nitekim bu saldırılar sonrasında, bahse konu küçük Baltık ülkesi, NATO'nun siber araştırmalar merkezi haline gelmiştir ve halihazırda Siber Savunma Mükemmeliyet Merkezi'ne ev sahipliği yapmayı sürdürmektedir.

SONUÇ

Anglo-Amerikan literatürde 'attribution' olarak geçen, bir saldırının kaynağının tespit edilmesi problemi siber güvenlik, siber savunma ve –henüz gelişmekte olan– siber harp alanlarında en ciddi sorun olmayı sürdürmektedir. Bu çalışmanın birçok yerinde alıntılandığı üzere, gerek pratikte gerek akademik düzeyde 'tespit edilmesi gereken kaynağın' bizatihi ne olduğuyla ilgili dahi bir konsensüs sağlanmış değildir. Zira, siber intrüzyonun giderek çok katmanlı (multi-stage) bir hal alması, kaynağın izini teknik imkanlar ile 'bilgisayara doğru' mu, insan istihbaratı da (HUMINT) dahil olmak üzere klasik istihbarat yöntemleri ile 'kişi ya da kişilere doğru' mu, yoksa siyasi-askeri mülahazalar ve stratejik istihbarat yaklaşımları ile olası yönlendirici devlet(ler)e doğru mu sürmek gerektiği hususunda bir görüş birliği yoktur. Esasen, böyle bir görüş birliği olması da mümkün görünmemektedir. Zira, tespit piramidi yukarı doğru çıktıkça, siyasi ve uluslararası hukuki mülahazalar teknik mülahazaların önüne geçmektedir. Hatta, bir siber saldırının devlet düzeyinde bir aktöre isnat edilmesine karşın sonuç alıcı ve somut gelişmelerin olmaması halinde, siber güvenlik alanında caydırıcılık zarar dahi görebilir. Dolayısıyla, tespit edilen bulguların diplomatik kanallar ile deklare edilip edilmemesi de ayrı bir siyasi tercih olarak karşımıza çıkmaktadır.

Siber saldırıların tespiti alanında bir diğer sorun da, siber-uzayın fiziksel niteliklere sahip bir ortam olmamasından ötürü uluslararası hukuktaki ülke egemenlik sahası ve sınırlar gibi kavramları tam olarak karşılayamamasıdır. Bu çalışmada alıntılanan hayali bir senaryoda belirtildiği üzere, devlet düzeyinde bir aktöre yakın hacker grubunun-bahse konu devletin vatandaşı olmayan-bir üyesi, olay ile ilgisi olmayan üçüncü ülke toprağından, farklı bilgisayarlardan zincirleme olarak yararlanmak suretiyle devlet düzeyindeki başka bir aktörün milli güvenlik açısından hassas bilgilerine erişebilir ya da sistemlerine siber saldırı düzenleyebilir. Sadece bu vakanın soruşturmasında yaşanacak gerek teknik gerekse hukuki karmaşa dahi, tespit / isnat sorunsalının karmaşık profilini açıklamaya yetecektir. Soruşturmanın ulaştığı bulguların nasıl ve hangi koşullar ile açıklanacağı ya da açıklanamayacağı ise siyasi bir karar olacaktır.

Yine de, siber alanda devlet ve devlet-dışı gruplara ilişkin 'sorumlu tutma' zeminindeki kaçınılmaz gereklilik henüz tam olarak ortaya çıkmış değildir. Evet, ABD, Güney Kore, İran, Estonya, Ukrayna ve Gürcistan gibi uluslararası sistemin birbirlerinden çok farklı birçok ülkesi değişik kontekst ve koşullarda siber saldırılara maruz kalmıştır. Yine de, kritik ulusal altyapıya geri dönülmez şekilde zarar veren, milli kapasiteyi çökerten, devletlerin bağımsızlık yeteneklerini doğrudan tehdit eden ve çatışmanın gidişatını karakteristik biçimde değiştiren bir siber harp durumu henüz yaşanmamıştır. Bu nedenle de, siber saldırılara konvansiyonel olarak ya da stratejik silah sistemleriyle mukabele etmek gibi bir seçenek ciddi karşılık bulmuş değildir. Ancak, gelişen teknoloji ve daha da önemlisi, birçok gelişmiş devletin altyapılarının giderek daha çok dijitalize olması yukarıda anılan olasılığı güçlü kılmaktadır. Siber harp, 2000'li yılların başında henüz somut bir gerçeklik olmayabilir. Öte yandan, yapılan projeksiyonlar, önümüzdeki on yıllarda söz konusu ihtimalin hafife alınmaması gerektiğini göstermektedir. İşte bu durum, yani tam manasıyla siber harp vakası gerçekleşir ise, siber saldırıların tespiti ve sorumluluk isnatı ucu stratejik silah sistemlerine dayanan bir tırmanmaya varabilecek uluslararası krizleri engelleyen ya da tetikleyen unsurlara dönüşebilecektir.

[52] Ibid.

[53] Ibid.

Ekonomi ve Dış Politika Araştırmalar Merkezi

edam

Siber Politikalar ve Dijital Demokrasi 2017/4

Aralık 2017

Hayaletlerin İzlerini Sürmek: Uluslararası Nitelikteki Siber Saldırıların Soruşturulması

Dr. Can Kasapoğlu | EDAM Savunma Analisti