



Bilgi Savasının



Sosyal Yikim Uclusu



CEVIREN

GUCLU AKPINAR

Bilgi-Savaşı'nın 'Sosyal Yıkım Üçlüsü' Nasıl Yenilir?

“Savaşın kuralları” değişti. Askeri olmayan araçların siyasi ve stratejik hedeflere ulaşmadaki rolü büyüdü ve çoğu durumdada, etkinliklerinde silahların yıkım gücünü aştılar.”

— Rusya Genelkurmay Başkanı Orgeneral Valery Gerasimov,

Askeri-Endüstriyel Kurier, Şubat 2013

"Rusya, bilgi savaşı tarihinde gördüğümüz en etkileyici bilgi savaşını yıldırım harekati konseptinde yürütüyor."

— General Philip Breedlove, NATO Galler Zirvesi, Eylül 2014

Bu zirveden yedi yıl sonra Amerika, modern bilgi savaşında üç unsurdan yararlanan daha becerikli bir Rusya ile karşı karşıya: bu uc unsur sirasi ile 1.sosyal medya, 2.propaganda/sahte haberler ve 3.dijital sosyal mühendislik – “bu unsurlari sosyal yıkım üçlüsü olarak adlandirabiliriz”. Üçlünün ileri düzeydeki kalıcı tehdidi, ulusal güvenlik için çok açık ve halihazirda geçerli bir tehlikedir, çünkü ulus-devletler ve terör örgütleri, sosyal medya teknolojisinin her yerde bulunan gücünü kullanmayı ve dijital toplum mühendisliği sanatı aracılığıyla kitleleri manipüle etmek için profesyonel bilgi savaşçılarını kullanarak propaganda ve sahte haberler "ureterek kitlelere iletmeyi" öğrendiler.

ABD hükümeti ve özellikle Savunma Bakanlığı, bu bilgi silahlarının kullanimindan kaynaklanan benzeri görülmemiş zorluklarla karşı karşıya.

Ulusal güvenlik uzmanı Clint Watts, “**Düşmanla Icice**” adlı kitabında açıkça “Amerika bilgi savaşında berbat, kesinlikle berbat” diyor. Ülke, kinetik silah sistemleri geliştirmek için muazzam çaba harcarken, rakibinin Triad of Disruption stratejisi için henüz kapsamlı bir savunma planı geliştirmedeği açık.

Şekil bir, üç unsurun Sosyal Yıkım Üçlüsünü oluşturmak için nasıl etkileşime girdiğini ortaya koymaktadır. Nihai amaca, Amerikan toplumunun kaosa sürüklenmesine yol açan bir kitle imha silahı olarak görülebilecek, nüfuz, istikrarsızlaştırma ve yıldırma savaşında kullanılan bu sosyal yıkım uclusunun birleşik gücüdür.

Sosyal Yıkım Üçlüsünün gücünü takdir etmek için, her bir unsurun silahı geliştirmedeki rolünü anlamanız gerekir.

Silahı, mesaj iletimi olan sosyal medya, toplumun her alanında kendini değiştirmeye devam ediyor.

Bugüne kadar, sosyal medya sitelerine öz polis propagandasına veya sahte haberlere güvenmek etkisiz kalmıştır. 1996 İletişim Ahlakı Yasası'nın 230. Bölümü sadece 26 kelimeye sahiptir. Bölüm 230, "Hiçbir etkileşimli bilgisayar hizmeti sağlayıcısı veya kullanıcısı, başka bir bilgi içeriği sağlayıcısı tarafından sağlanan herhangi bir bilginin yayıncısı veya sözcüsü olarak muamele görmeyecektir." medya platformlarının kullanımı.

Değişiklik gerektiren kusurlu bir yasadır; özellikle, ifade özgürlüğü ve sorumlu çevrimiçi sosyal katılım arasındaki dengeyi bulmak için iki partili mevzuat gereklidir. Bu konuyu ele almadan, sosyal medya platformlarının bir saldırı vektörü olarak kullanılmaya devam edilmesinin öngörülebilir gelecek için sınırı yok gibi görünüyor.

Sırada propaganda ve yalan haberler var. Uluslara, kuruluşlara veya bireye zarar vermek amacıyla söylenti, fikir, bilgi ve yalanların yayılması propagandadır ve "bilgi manipülasyonu" unsurudur. Yüzlerce yıldır kötülük amacıyla başarıyla kullanılmıştır. Adolf Hitler'in yükselişini desteklemek için Naziler, kötülüklerini Alman toplumunun her yönüne aşılarken propagandayı bir sanat biçimine dönüştürdüler.

Propaganda tarih boyunca ne kadar tehlikeli ve etkili olursa olsun, sosyal medyanın ortaya çıkışı tehdidi kat kat artırıyor. Üç Aylık Stratejik Araştırmalarda Yazan Hava Kuvvetleri Komutanı Yarbay Jarred Prier, "**Eğilime Komuta Etmek: Bilgi Savaşı Olarak Sosyal Medya**" başlıklı makalesinde, bu

artan kontrolsüz propaganda tehdidine ve dijital ortamda yayılmasına katkıda bulunan ilgili niteliklere değindi.

Bu ölümcül kombinasyonu ve farklı teknoloji araçlarının, oyuncuların ve mesajlaşmanın, temsili sosyal medya platformu Twitter'ı kullanarak propagandaya inanılmaz dayanıklılıkla bir ömür sağlamak için nasıl birleştiğini yansıtıyor.

Propagandanın birincil uğursuz ortağı sahte haberlerdir. Sahte haberler, bu yeni silahın anlaşmazlık çıkarma, yalanları etkinleştirme ve motive etme yeteneğini tamamlamak için enerji kaynağı olarak hizmet ediyor.

Yalan haber yeni bir terim değildir; ve son zamanlarda değişime uğramış kullanımı orijinal anlamından farklıdır. Ne yazık ki, sahte haberler kendi başına bir endüstri haline geldi. Artık bazı önde gelen politikacıların beğenmedikleri haberleri indirgeme yöntemi olarak favori bir teknik.

Kaynak, yalnızca alıcının siyasi görüşüne dayalı olarak güvenilir olarak kabul edilmediğinden, olgusal olarak kanıtlanabilir konular genellikle sahte haber olarak etiketlenir.

Diğer bir faktör de dijital sosyal mühendisliğin yükselişidir. Sosyal mühendis Christopher Hadnagy, alanını **"bir kişiyi, hedefin çıkarına olabilecek veya olmayabilecek bir eylemi gerçekleştirmesi için manipüle etme eylemi"** olarak tanımlar.

Sosyal mühendislik, basitçe, başkalarını istediğiniz şeyi yapmalarını sağlamak için manipüle etme sanatıdır. Bununla birlikte, bu beceriyi çevrimiçi teknoloji ile birleştirmek, dijital sosyal mühendisliğin gücünü üretir – "sosyal nedenler planlama stratejisi" ögesi.

Sosyal mühendislik sanatı insanlar kadar uzun süredir var olsa da, dijital çağın gelişi saldırganla daha hızlı sonuçlarla daha geniş bir hedefe ulaşma yeteneği sağlıyor. Rus toplum mühendisleri, sadece on yıl önce hayal bile edilemeyecek bir şekilde Amerika Birleşik Devletleri'ne saldırmak için inşa

edilen silahın bu son parçasının temsilcileridir.

2017 Ulusal İstihbarat Direktörü ve 2020 ABD Senatosu İstihbarat Komitesi raporları, 2016 ABD başkanlık seçim kampanyası sırasında Rus İnternet Araştırma Ajansı'nın (IRA) Sosyal Yıkım Üçlüsünü kullanmadaki eşi görülmemiş başarısını özetledi.

Rusya'nın saldırısının ABD'nin ulusal güvenliğini etkilediğine şüphe yok. Ek olarak, IRA'nın siyasi kaosa neden olan düşük yatırım maliyetli/yüksek getiri stratejisi, ABD vatandaşları arasındaki uluslararası ittifaklar ve anlaşmazlıkların kullanılması, askeri tarihteki en başarılı uzun vadeli yüksek yatırım getirisi olan saldırılarından biri olarak tanımlanacaktır.

2016'dan sonra Rusya, endişe verici derecede açık bir Triad of Disruption stratejisini sergileyerek fayda sağlamaya devam etti. Gürcistan, Ukrayna, Fransa, Büyük Britanya ve diğer ülkeler IRA saldırı stratejisinin hedefi oldular. Yine de, Rusya'nın yıllarca "dijital" bombardımanından sonra, Amerika ve müttefikleri bu silahı yenmek için henüz bir karşı-denge stratejisi bulabilmiş değiller.

Diğer rakipler Rusya'nın başarılarını fark ettikleri için, neredeyse anlamlı bir ceza olmadan, onlar da rakiplerine karşı Sosyal Yıkım Üçlüsünü uyguluyorlar. Çin, Kuzey Kore ve İran bilgi savaşı faaliyetlerini artırıyor. Terör cephesinde, IŞİD sosyal medyayı sofistike kullanımıyla zaten biliniyordu ve IRA'nın stratejilerini incelediklerine ve savaş planlarını geliştirdiklerine şüphe yok. gelecekteki bilgi savaşı saldırıları.

Bir Ulus, Sosyal Yıkım Üçlüsüne karşı kendini nasıl savunabilir?

Pentagon'un Sosyal Yıkım Üçlüsüne karşı etkili bir savunma inşa etme mücadelesi, karşılaştığı her şeyden daha karmaşık ve benzersizdir. Cevap yeni bir silah sistemi inşa etmek değil - gerçek şu ki, bu silaha karşı en iyi savunma eğitim, iyi politika, etkili yasalar, kamu-özel sektör ortaklıkları ve uluslararası ittifaklar ve anlaşmalardır.

Savunma Bakanlıđının bu tehdide tek başına karşı koyamayacağını anlamak zorundadır. Karşı koyma cabalarının etkin olması her düzeyde hükümet, özel sektör ve üniversite katılımını gerektirir.

Bu nedenle, aşağıdaki savunma planı, hükümet çapında bir "tüm unsurların biraradalığını içeren" bir taahhüt gerektirir. İlk olarak, Savunma Bakanlığı, tüm Amerikalılar için daha okulun ilk günlerinde ve yetişkinlik boyunca devam edecek bir siber güvenlik eğitim programına yönelik hükümet çapında bir taahhüdü finanse etmek ve desteklemek için diğer kurumlarla ortaklık yapmalıdır.

Hükümet, özellikle Bölüm 230 ile ilgili olarak, sosyal medya için özel sektör standartlarına ilişkin yasa ve politikaların etkinliğini yeniden gözden geçirmelidir. Ardından, özel askeri yükleniciler ve akademik topluluklar, tanımlayan ve karşı koyan teknik süreçler geliştirmek için kamu-özel ortaklıkları aracılığıyla hükümetle birlikte çalışmalıdır. derin sahtekarlıklar ve diğer ortaya çıkan dijital sosyal mühendislik yöntemleri gibi saldırılar.

Pentagon, çevrimiçi bilgi savaşı tekniklerinin tespiti, tanımlanması ve doğrulanmasına yönelik daha fazla kaynak ayırmalı. Bu sadece teknoloji ile yapılamaz.

Ayrıca, topluluğun bu gelişen silahı kültürel ve sosyal olarak nasıl kavramsallaştırdığı konusunda bir değişiklik gerektiriyor. Tüm hükümet seviyeleri, her Amerikalı'nın Yıkım Üçlüsü'nün unsurları hakkındaki anlayışını geliştirmeli ve taahhüt etmelidir. Buna, 1970'lerde başlatılan sigara karşıtı kampanyaya benzer kapsam ve genişlikte bir ulusal bilinçlendirme kampanyası oluşturulması da dahildir. Amerikalıların bu silahı anlamaları gerekiyor, böylece onlar da ulusun birleşik savunmasında rol oynayabilirler.

Son olarak, Savunma Bakanlığı, konsept olarak ABD-Rusya nükleer anlaşmalarına benzer bir uluslararası siber güvenlik anlaşmasını

desteklemelidir. Sonuç, tüm uluslar için geçerli olan uluslararası bir siber güvenlik sözleşmesi olacaktır.

Böyle bir anlaşmayı uygulamak için Amerika Birleşik Devletleri, bağımsız izleme, adli soruşturma ve tanımlama için yasal yetkiye ve Triad of Disruption silahını kullanmaktan suçlu ülkelere karşı cezai işlemler uygulama yeteneğine sahip bir Birleşmiş Milletler siber güvenlik teşkilatının kurulmasını desteklemelidir.

Sosyal Yikim Üçlüsü'nün unsurları, ulus devletlere ve terörist gruplara bir hedefe karşı düşük risk veya maliyetle büyük ölçekte bilgi savaşı yürütme yeteneği sağlayan olağanüstü güçlü bir silah oluşturmak için birleşir.

ABD'nin 2016 başkanlık seçimlerine yönelik Rus saldırısı, tarihte bu üçlüyü kullanan en etkili saldırıydı, ancak uzun sürmeyecek. ABD' nin düşmanları, internet ve sosyal medya teknolojilerini kullanarak ulusa yıkıcı sonuçlarla saldırmak için profesyonel dijital sosyal mühendislerden yararlanarak zarar verici propaganda ve sahte haberler yayma yeteneğine sahiptir.

Sosyal Yikim Üçlüsü, Amerika için açık ve mevcut bir tehlikedir. Bütün bir ulusun savunmada seferber olmasını gerektirir.

How to Defeat the Info-Warfare 'Triad of Disruption'

"The very 'rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."

— Gen. Valery Gerasimov, Russia's chief of the general staff,

Military-Industrial Kurier, February 2013

"Russia is waging the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."

— Gen. Philip Breedlove, NATO Wales Summit, September 2014

In Seven years later, America faces a more skillful Russia experienced in modern information warfare leveraging three elements: social media, propaganda/fake news and digital social engineering — the "triad of disruption." The advanced persistent threat of the triad is a clear and present danger to national security because nation-states and terrorist organizations have learned to apply the ubiquitous power of social media technology, and "message" propaganda and fake news utilizing professional information warriors to manipulate the masses via the art of digital social engineering.

The U.S. government, and the Defense Department specifically, faces unprecedented challenges from this information weapon. In his book, "Messing with the Enemy," national security expert Clint Watts bluntly states that "America sucks at information warfare, absolutely sucks." While the nation expends tremendous effort to develop kinetic weapon systems, it is clear it has yet to develop a comprehensive defense plan for its adversary's Triad of Disruption strategy.

Figure one reveals how the three elements interact to produce the Triad of Disruption. It is the merged power of the overlapping elements used in the battle of influence, destabilization and intimidation that manifests as a weapon of mass destruction leading to the ultimate goal — the decline of American society into chaos. To appreciate the power of the Triad of Disruption, one needs to understand each element's role in developing the weapon.

The weapon's message delivery element, social media, continues to morph itself across every aspect of society. To date, relying upon social media sites to self-police propaganda and fake news has been ineffective. Section 230 of the 1996 Communications Decency Act has but 26 words. Section 230 reads, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." It is a blanket protection for social media providers from legal action as a result of the use of their media platform.

It is a flawed law requiring change; specifically, bipartisan legislation is required to find the balance between freedom of speech and responsible online social engagement. Without addressing this issue, the continued use of social media platforms as an attack vector seems to have no boundaries for the foreseeable future.

Next is propaganda and fake news. The spreading of rumors, ideas, information and lies in order to cause harm to nations, organizations or an individual is propaganda and is the "information manipulation" element. It has been used successfully for hundreds of years for purposes of evil. To support Adolf Hitler's ascendance, the Nazis honed propaganda to an art form as they instilled their evil into every aspect of German society.

As dangerous and effective as propaganda has been throughout history, the introduction of social media amplifies the threat many-fold. Writing in a Strategic Studies Quarterly article, "Commanding the Trend: Social Media as Information Warfare," Air

Force Lt. Col. Jarred Prier addressed this growing threat of unchecked propaganda and related attributes which contribute to its spread in the digital environment.

Figure 2 reflects this lethal combination and how the different technology tools, players and messaging combine to give propaganda a lifespan with amazing stamina using the representative social media platform, Twitter.

The primary sinister partner to propaganda is fake news. Fake news serves as the energy source to complete this new weapon's ability to sow discord, enable lies and motivate believers. Fake news is not a new term; and its recently mutated use is not the original meaning. Unfortunately, fake news has become a cottage industry to itself. It is now a favorite technique of some prominent politicians as a method to discount any news they don't like. Issues that are factually provable are often tagged as fake news because the source is not considered credible solely based upon the receiver's political persuasion.

Another factor is the rise of digital social engineering. Social engineer Christopher Hadnagy defines his field as "the act of manipulating a person to take an action that may or may not be in the target's best interest." Social engineering is simply the art of manipulating others to get them to do what you want.

However, combining that skill with online technology produces the power of digital social engineering — the "pretext planning strategy" element. And, while the art of social engineering has been around as long as humans, the advent of the digital era provides the attacker the ability to reach a more expansive target set with rapid results. Russian social engineers are representative of this final piece of the weapon built to attack the United States in a manner unimaginable just a decade ago.

The 2017 Director of National Intelligence and the 2020 U.S. Senate Intelligence Committee reports outlined the unprecedented success of the Russian Internet Research Agency (IRA) in its use of the Triad of Disruption during the 2016 U.S. presidential election campaign.

Without a doubt, Russia's attack had an impact on U.S. national security. Additionally, the IRA's low investment costs/high-yield return strategy to cause political chaos, weaken international alliances and sow discord among U.S. citizens may be one of the most successful long-term return on investment attacks in the annals of military history.

After 2016, Russia continued to reap benefits as it flaunted an alarmingly open Triad of Disruption strategy. Georgia, Ukraine, France, Great Britain and other nations have been targets of the IRA attack strategy. And yet, after years of "digital" bombardment by Russia, America and its allies have yet to find a counter-balance strategy to defeat this weapon.

As other adversaries have recognized the successes of Russia, almost without meaningful penalty, they too are applying the Triad of Disruption against their rivals. China, North Korea and Iran are increasing their information warfare activities. On the terrorism front, ISIS was already known for its sophisticated use of social media, and there can be no doubt they have studied the IRA's strategies and are honing their battle plans for future information warfare attacks.

How can the nation defend itself against the Triad of Disruption?

The challenge to the Pentagon in building an effective defense against the Triad of Disruption is more complex and unique than any it has confronted. Building a new weapon system is not the answer — the fact is that the best defense against this weapon is education, good policy, effective laws, public-private partnerships, and international alliances and treaties.

It is imperative to understand that the Defense Department cannot counter this threat by itself. It requires all levels of government, private industry and academia.

As such, the following defensive plan requires an “all-in” government-wide commitment.

First, the Defense Department should partner with other agencies to fund and support a government-wide commitment to a cybersecurity education program for all Americans as early as the first days of school and continuing throughout adulthood.

Government should revisit the efficacy of laws and policy regarding private industry standards for social media, especially in regard to Section 230. Next, private military contractor and academic communities should team with the government via public-private partnerships to develop technical processes which identify and counter attacks such as deep fakes and other emerging digital social engineering methods.

The Pentagon should dedicate more resources toward detection, identification and authentication of online information warfare techniques. This cannot be done by technology alone.

It also requires a change in how the community conceptualizes this evolving weapon culturally and socially. All levels of government should develop and commit to every American’s understanding of the elements of the Triad of Disruption. This includes establishing a national awareness campaign similar in scope and breadth to the anti-smoking campaign begun in the 1970s.

Americans need to understand this weapon so they too can play a role in the nation's combined defense.

Finally, the Defense Department should support an international cybersecurity treaty similar in concept to the U.S.-Russia nuclear treaties. The result would be an international cybersecurity convention applying to all nations.

To enforce such a treaty, the United States should support the establishment of a United Nations cybersecurity agency with the legal authority for independent monitoring, forensic investigation and identification, and the ability to impart punitive actions against countries guilty of wielding the Triad of Disruption weapon.

The elements of the Triad of Disruption merge to form an extraordinarily powerful weapon providing nation-states and terrorist groups with the capability to execute information warfare against a target on a massive scale, at low risk or cost.

The Russian attack against the United States' 2016 presidential election was the most effective attack using the triad in history, but it won't be for long. U.S. adversaries are capable of propagating damaging propaganda and fake news, utilizing the technologies of the internet's social media, and then leveraging professional digital social engineers to attack the nation with devastating results.

The Triad of Disruption is a clear and present danger to America. It requires an entire nation to mobilize in defense