BİLGİ HARBİNDE KAZANAN AZERBAYCAN

AZERBAIJAN WON THE INFORMATION WAR

Konul MEMMEDOVA

Nahçıvan Devlet Üniversitesi, memmedovak1976@gmail.com,

https://orcid.org/0009-0003-9316-3203

Annagi ASGAROV

Nahçıvan Devlet Üniversitesi, askerov197@mail.ru,

https://orcid.org/0009-0004-1767-2863

ÖZET

Makale, komuta ve kontrol, istihbarata dayalı, psikolojik, ekonomik bilgi, elektronik, bilgisayar korsanlığı ve siber silahlar gibi çeşitli Bilgi Güvencesi biçimlerini açıklamadan önce Bilgi Güvencesine bakıyor. Buna ek olarak, makale, Bilgi Savaşının dört ilkesini özetlemekte ve dört temel strateji kullanılarak herhangi bir hedefe ulaşmak için silahların nasıl kullanılabileceğini incelemektedir: Bilginin Reddi, Aldatma ve Taklit, Tehdit, İmha ve Yıkım. Makale, bilgi savaşları sırasında bilgi üstünlüğünü sağlamanın önemli olduğunu göstermektedir. Ortaya çıkan bu durumla ilgili sürekli bilgi akışını toplama, kontrol etme ve yayma yeteneği, bir düşmanın benzer bir girişimde bulunmasını engelleme yeteneği olarak tanımlanmaktadır. Bilgi ağı savaşını yürütmek daha kolay hale gelir ve negatif, anonim bilgilerin kontrolsüz şekilde yerleştirilmesi olasılığını yaratır. Makalede ayrıca tarihte bilinen en büyük siyasi ve askeri hataların, düşmanın moralinin yanlış değerlendirilmesi nedeniyle gerçekleştiği vurgulanıyor. Herhangi bir harekât sahasındaki düşman birliklerinin morali, geleneksel istatistiksel hesaplamalarla ve savaş esirlerinin küçük bir örneğinin incelenmesiyle değerlendirilebilir. Mahkûmların yokluğunda, bilgi verilerinin analizine, düşmanın birliklerine ve halkına yönelik propagandaya dayanarak neredeyse aynı sonuçlara ulaşılabilir. Bu, düşman birliklerinin belirli bir durumdaki davranışlarını tahmin etmenizi sağladığı göz önüne çıkarılır.

Anahtar kelimeler: Bilgi, tehlike, savaş, elektronik, teknoloji

ABSTRACT

The article first looks at Information Assurance before describing the various forms of Information Assurance such as command and control, intelligence-based, psychological, economic information, electronic, hacking and cyber weapons. In addition, the article outlines the four principles of Information Warfare and examines how weapons can be used to achieve any goal using four key strategies: Denial of Information, Deception and Impersonation, Threat and Destruction, and Subversion. The article shows that it is important to maintain information superiority during information wars. The ability to collect, control and disseminate the constant flow of information regarding this situation is defined as the ability to prevent an attacker from making a similar intervention. It becomes easier to conduct cyber warfare, creating the possibility of uncontrolled placement of negative, anonymous information. The article also emphasizes that the biggest political and military mistakes known in history occurred due to incorrect assessment of the enemy's morale. The morale of enemy troops in any theater of operations can be assessed by conventional statistical calculations and by examining a small sample of prisoners of war. In the absence of prisoners, almost the same conclusions can be reached based on the analysis of information data, propaganda against the enemy's troops and people. This allows you to predict the behavior of enemy troops in a given situation.

Key words: İnformation, danger, war, electronics, technology

1. GİRİŞ

Bilgi güvenliği nedir? Bu sorunun doğru bir cevabı olmayacak. Farklı geçmişlere sahip insanlar farklı cevaplar verecektir; muhtemelen ne tür bir işin içinde olduklarını açıklamaya çalışıyorlar. Halk, Bilgi Savaşını kritik bilgilerin rakiplerine ulaşmasını engelleme girişimi olarak algılayabilir. Bunu yapmak, rakiplerinin işlerini tehlikeye atmadan, yeteneklerini yavaşlatacaktır. Genel halk bunu internette "savaş" olarak görebilir, ancak askeri açıdan başka bir anlama gelebilir.

Bilgi savaşı, askeri ve ya genel halk içinde savaş yürütmek için ayrı bir teknik değildir. Daha büyük bir konsept oluşturmak için bir araya gelen farklı formlardan oluşur. Martin Libicki (1995) yedi bilgi sağlama biçimini şu şekilde tanımlamıştır:

- Komuta ve Kontrol Güvenliği (C2W),
- Akıllı Tabanlı Harp (IBW),
- Elektronik Koruma (EW),
- Psikolojik Savaş (PW),
- Ekonomik Bilgi Koruması (EIW),
- Anti-hacker (HW) ve
- Siber Harp (CW)

Bilgi Savaşının İlkeleri

Daniel E Magsig (1996), Bilgi Savaşının ilkelerini şu şekilde sıralamıştır:

- Reddetme,
- Artan güç,
- Yaşanabilirliği sağlamak için Yerelleştirme, Kontrol, İletişim
- Seviye.

Düşmanın, kendisinin ve dost kuvvetlerin güçlü ve zayıf yanlarını bilmek, bir savaşı kazanmak için esastır. Bu bilgilerin muhalif komutanlara verilmemesi onları karanlıkta bırakacaktır. Bu nedenle, komuta ve kontrol merkezleri, karar destek ve iletişim sistemleri birincil hedefler olmalı ve savaşa girmeden önce tüm düşman sensörleri bastırılmalı ve ya imha edilmelidir.

İkinci ilke, Gücün artmasıdır. Komutanları kadar karadaki birliklerin de bilgiye ihtiyacı var. Birliklere yönelik ek riskleri azaltmak veya önlemek için yukarıdan aşağıya bilgi akışı mümkün olduğunca sorunsuz olmalıdır.

Yaşanabilirliği sağlamak için yerelleştirme esastır. Politika ve strateji en üst düzeyde merkezileştirilmeli, ancak alt düzeyin kendi misyonlarını planlamasına ve yürütmesine izin verilmelidir. Canlılığı sağlayan bir diğer husus birlikte çalışabilirliktir. Maksimum bilgi alışverişinin yapılabilmesi için tüm bilgi ve iletişim sistemlerinin birbiriyle konuşabilmesi gerekir.

Bilgi Savaşının son ilkesi olan Düzey, düşmanın yeteneklerinden bağımsız olarak, mevcut tüm teknolojinin düşman kuvvetlerine karşı kullanılması gerektiğini belirtir. Bilgi savaşı çatışmalarını yoğunlaştırmak için her türlü çaba gösterilmelidir.

Kriptoloji

Kriptoloji, sırasıyla güvenli iletişimleri şifrelemek ve kırmak için tasarlanmış bir bilgi savaşı silahıdır.

Kriptografideki önemli ilerlemelere rağmen, kriptanaliz, bilgi işlem gücündeki eşit derecede önemli ilerlemelerle desteklenen önemli bir silah olmaya devam edecektir.

Videoyu değiştirme

Video kurcalama, güvenilirliği baltalamak için bir düşman liderinin söylemediği şeyleri söylemiş gibi görünmesini sağlamak için kullanılabilecek bir silahtır.

Bilgi savaşında temel stratejiler

Bilgi Savaşı İlkeleri, bir bilgi savaşını kazanmak için ne yapılması gerektiğini açıklar. Buradaki stratejiler bunun nasıl yapılacağını açıklar. Dört ana strateji aşağıdaki gibidir (Copp, 2000):

- Bilgi Reddi
- Aldatma ve Kimliğe Bürünme
- Tehlike ve Yıkım
- Provokasyon

Bir kullanıcı, diğer tarafın kritik verilerine erişmesini istemez. Güvenlik duvarları, İzinsiz Giriş Tespit sistemleri, Sanal Özel Ağlar, şifreleme ve daha yakın zamanlarda steganografi kullanımı, düşman kuvvetlerinin verilerine erişimini engelleme girişimlerinin tezahürleridir. Aynı zamanda bilgisayar korsanları, teröristler ve yabancı ülkeler, yanlış bilgi veya yazılım eklemek, işlev bozukluğuna ve dolayısıyla doğrudan yıkıma neden olmak amacıyla düşmanın bilgi sistemlerinin çekirdeğine girmek için her gün yeni araçlar geliştiriyorlar.

Sabotaj, bilgilerin bir rakibin sistemine enjekte edildiği ve sistemin kendisine zarar vermek için sistem kaynaklarını kullanan bir mantık bombası, virüs ve diğer yıkıcı programlar gibi kendi kendini yok eden bir sürece neden olduğu bir stratejidir.

Azerbaycan ile Ermenistan arasında yıllardır süregelen, Sovyet iktidarının dağılmasının ardından yeniden gündeme gelen ve 30 yıldır nefret ettiğimiz komşularımız tarafından işgal altında tutulan Dağlık Karabağ sorunu, İç Savaş ile hakkaniyetli çözümünü bulmuştur. 27 Eylül 2020'de başlayan ve 44 gün sonra sona eren...

Zaferimizin sebebi, hem cephede hem de cephede halkımızın birliğiydi. Ermeni tarafı kendi halkına asılsız bilgiler aktarıyor, bu yanlış bilgileri yayarak savaşı kazanacağını sanıyordu. Bu, ülkemizin vatansever insanlarını endişelendirdi. Bu konuyla ilgili olarak Azerbaycan, Ermenistan'da

bir sosyal medya botu oluşturdu. Buna "TAVUSH BOT" adı verildi. Amaç Ermeni halkına doğru bilgiyi ulaştırmak, Ermenilerin yürüttüğü bilgi savaşının ne kadar ölçüsüz olduğunu kanıtlamak ve düşmanı bu cephede de yok etmekti. Peki "Tavuş Botu" neydi? "Tavush Bot", kendi kendini ilan eden ilk yapay zekâ Ermeni sosyal medya botuydu. "Tavush Bot" ilk kez Temmuz muharebelerinin arifesinde "Tavush" bölgesinde yaşayan insanlara doğru bilgileri ulaştırmak için oluşturuldu. "Tavush Bot" Ermenice bilen ve Google Asistan mantığıyla çalışan yapay zekâ tabanlı bir bottu. Bu bot Ermenilerle konuşuyor, bilgilerini topluyor ve gerektiğinde onlara toplu mesajlar gönderiyordu. Tavush Bot adlı sosyal ağ programının yazarı, çok sayıda teknoloji ve startup projesinin yazarı Farid Pardaşunas'tı.

44 gün süren Vatanseverlik Savaşı sırasında Ferid Pardaşunas'ın büyük etkinliği Azerbaycan'ın sosyal medyasında yer aldı. Farid Pardaşunas'ın ileri yüksek teknolojilerin ve yenilikçi fikirlerin uygulanmasıyla girişimcilik faaliyetinin uygulanmasındaki başarılarının yanı sıra Azerbaycan Cumhuriyeti Cumhurbaşkanı Kararnamesi ile 2021 Cumhurbaşkanlığı Gençlik Ödülü'ne layık görülmesi tesadüf değildir. Gençler arasında bu etkinliğin tanıtımı ve tanıtımı alanı.

Günümüzün yeni muharebe alanlarında bilgisayarlar ve sistemler üzerinde yürütülen enformasyon savaşının bugüne kadar genel bir tanımı bulunmamaktadır. Bilgi savaşının ilk teknik tanımı ilk olarak John Alger tarafından rapor edildi. Bu bağlamda bilgi savaşı, bilgimizi ve bilgi tabanlı yapılanmamızı korurken, düşmanın bilgi, bilgi sistemleri ve bilgi tabanlı yapılarını etkileyerek bilgi avantajımızı elde etmemizi sağlayacak her türlü faaliyeti ifade eder. Benzer bir tanım ABD Hava Kuvvetleri tarafından verildi. Bu tanıma göre, bilgi savaşı, bir rakibin bu faaliyete karşı harekete geçmesini önlemek ve hasım bilgilerine ve işlevlerine müdahale etmek için benzer operasyonlara karşı koyma, yok etme ve bunlardan yararlanma eylemidir. Leeds Üniversitesi İletişim Enstitüsü'nde görev yapan Profesör Philip M. Taylor, bilgi savaşıyla ilgili düşüncelerini şöyle açıklıyor: "Dışarıda bir savaş var, bir dünya savaşı var ve bu savaş kimin daha fazla mermisi olduğu, bizim nasıl savaştığımızla ilgili değil. Gör, duy, ne yaptığımızı ve ne düşündüğümüzü. Verileri kim kontrol ediyor" (Alberts, 1996).

Bilgi savaşı, teknolojinin teknolojiye karşı kullanılmasıdır; sırlar ve sırların çalınması hakkındadır. Bu bilgiyi bilgi sahiplerine karşı kullanmak, düşmanı onların bilgi ve teknolojisini kullanma yeteneğinden mahrum etmektir. Bilgi savaşı, zaman ve mekândan bağımsız olarak herhangi bir hedefe karşı yürütülebilir. Toplumun her katmanına yaymak için askeri, ekonomik, siyasi, ideolojik ve hatta dini sorunlara dayalı stratejik, taktik ve operasyonel hedeflere uygulanabilir. Bilgi savaşının aşağıdaki türleri vardır (Winn, 1994).

Siber savaş, başka bir ülkenin bilgisayar sistemlerine veya ağlarına zarar verme veya bozma eylemidir. Elektronik savaş, askeri terminolojide radyo dalgalarını ve bir ordunun savaşın sonucunda belirleyici bir rol oynama taktiksel teknolojik üstünlüğünü içeren bir terimdir. Genel olarak amaç, çeşitli teknikler uygulanarak elektromanyetik spektrumun düşman kuvvetleri tarafından kullanılmasının tamamen önlenmesi ve aynı zamanda dost kuvvetlerin askeri amaçlara en uygun şekilde kullanılarak maksimum faydanın sağlanmasıdır. Elektronik harp, elektronik destek, elektronik saldırı ve elektronik savunma olmak üzere üç ana bölümde incelenebilir.

Elektronik saldırı, düşman kuvvetlerinin elektromanyetik spektrumu, özellikle radyo dalgalarını ve radar frekans bandını kullanmasını engellemek için askeri güç ve teknolojik altyapıyı kullanır, navigasyon, hedef tespiti, izleme, telekomünikasyon ve istihbarat paylaşım yeteneklerini azaltır. Bir elektronik saldırı aktif veya pasif olarak gerçekleştirilebilir.

Düşman tarafından aktif elektronik saldırı için kullanılan frekans aralığını kapsayan, yüksek güçlü karıştırıcı radyolar yayınlayarak, düşman radyo/keşif operatörlerini veya radar alıcıları gibi elektronik cihazları aldatarak aynı frekans bandında elektronik veya insan dezenformasyonu yayınlayarak düşman radyo iletişimini bozar, transponder istasyonları. Özel uçaklarda yaygın olarak

kullanılan aktif dalga iptal yöntemleri ve elektromanyetik darbe bombası (EMP) kullanımı örnek verilebilir (Haeni, 1997).

44 gün süren Vatanseverlik Savaşı sırasında Özel Kuvvetler'in baş sancağı olan Şehit Cemal İsmayilov, Ermeni telsiz muhaberesine katılarak Ermeni generallerine geri çekilme emri verdi. Bu, Azerbaycan'ın hem cephede hem de bilgi savaşında kazandığı zaferin açık bir örneğidir.

SONUÇ

Bilgi savaşı tehdidi gerçektir. Özellikle bilgisayar ağı ortamında bu saldırıları gerçekleştirmenin maliyetinin düşük olması, savunmayı çok zor bir problem haline getiriyor. Bu durum bilgi teknolojisinin hızla yayılmasıyla daha da kötüleşiyor. Bağlantı ihtiyacı arttıkça ağlara daha fazla bilgisayar bağlandıkça güvenlik açıkları artacaktır. Bu durum göz önüne alındığında, sistemimizi felaket olaylarından korumanın bir yolunu bulmalıyız. İlk adım, organizasyonumuzdaki insanlar arasındaki tehditlerin doğasını ve özelliklerini daha iyi anlamaktır. Çünkü insanlar her zaman en zayıf halkadır.

KAYNAKÇA

Alberts, D.S. (1996). Defensive Information Warfare, NDU Press Book.

Deborah, R., & Gangemi, G.T. (1994). Computer Security Basics. O'Reilly & Associates

Haeni, R.E. (1997). Information Warfare – an introduction, January.

Kopp, C. (2000). Information Warfare, https://www.ausairpower.net/OSR-0200.html, 11.01.2024.

Libicki, M. (1995). What is Information Warfare, National Defense University.

Magsig, D.E. (1996). Information Warfare In The Information Age.

The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) Number 3210.01, dated 02 January 1996

US DoD, Joint Pub 3-13 Joint Doctrine for Information Operations, 9 October 1998.

Winn, S. (1994). Information Warfare. Chaos on the electronic superhighway, (Thunder's mounth press)