Uluslararası İlişkilerde Güvenlik Çalışmaları

Bahar 2021

XIII. Güncel Uluslararası Güvenlik Sorunları - IV

Siber Güvenlik

Siber Güvenlik

- 1980'lerde bilişim teknolojilerinde (*Information and Communication Technologies - ICT*) yaşanan ilerleme (bilişim devrimi)
- Bilişim: bilgi + iletişim
- Bilişim teknolojileri: Bilgiyi elektronik ortamda dijital olarak oluşturmamızı, saklamamızı, geri çağırmamızı, işlememizi, yaymamızı ve almamızı sağlayan teknolojiler. (ör. bilgisayar, cep telefonu, internet, uydu vs.)
- Bilişim devrimini hazırlayan teknik ilerlemeler:
  - Haberleşme teknolojisi (19. yy.'dan beri)
  - Bilgisayar teknolojisi (1940'lardan beri)
  - Ağ teknolojisi (1960'lardan beri)
- Hepsinin kökeninde askerî rekabet ve ihtiyaçlar önemli rol oynuyor
- 1980'lerden itibaren özelleşme, ticarileşme, ucuzlama, yaygınlaşma

İnternet'in Hikayesi

- **1958** – ABD Savunma Bakanlığı -> **İleri Araştırma Projeleri Ajansı (ARPA)**
- **1969** – ARPA -> **ARPANET** (UCLA – Stanford – UC Santa Barbara – Utah)
- **1983** – MILNET (ABD Askerî Ağı), ARPANET'ten ayrılıyor
- **1985** – **ABD Ulusal Bilim Vakfı (NSF)** -> **NSFNET** (akademik ve sivil bir ağ)
- **1990** – **NSFNET, ARPANET'in** yerini alıyor ve ticarileşmeye başlıyor.
- **1990** – CERN-> **World Wide Web** teknolojisini icat ediyor.
- **1993** – **Grafik temelli web tarayıcıları** yaygınlaşıyor -> **Mosaic**
- **1995** – NSFNET, yerini **ticari internet ağına bırakıyor**.

Siber Uzay

- Kavram, ilk kez William Gibson (1982) tarafından kullanılıyor.
- Siber Uzay (*cyber space*), yeryüzündeki ve uzaydaki **tüm bilişim sistemlerinin ve kullanıcılarının** çeşitli ağlar aracılığıyla **birbirine bağlanmasıyla** meydana gelen **sanal ortam**dır.
- Siber Uzay, 4 katmandan (*layers*) oluşur:
  - Fiziksel Katman: elektronik ve elektromanyetik altyapı (donanım)
  - Yazılım Katmanı: kodlar ve onlardan meydana gelen yazılımlar
  - İçerik Katmanı: donanım ve yazılım aracılığıyla oluşturulup saklanıp yayılan enformasyon
  - Düzenleyici Katman: yukarıdaki 3 katmanı kontrol etmek için geliştirilen hukukî düzenlemeler
- Devletlerin siber uzay üzerinde mutlak bir hakimiyetinden bahsedemiyoruz.

Siber Güç ve Siber Güvenlik

- **Siber güç**, siber ortamın elektronik olarak birbirine bağlı enformasyon kaynaklarını kullanarak istenilen sonuçları elde etme becerisidir. (J. Nye, 2011) -> yumuşak güç
- Devletçi ve sert güç odaklı perspektiften bakıldığında-> Siber güç, devletlerin **siber tehditlere karşı koyabilme** ve **siber uzayı operasyonel anlamda kullanarak** avantaj elde edebilme kabiliyetidir.
- Bilişim sistemlerinin yaygınlaşması -> siber tehdit temsillerinin artması -> siber uzayın güvenlikleştirilmesi -> siber güvenlik -> ulusal güvenlik
- En temel ve en eski siber tehdit unsuru: **kötü amaçlı yazılımlar** (*malware*) ve onları yazıp kullanan **bilgisayar korsanları** (*hacker*)

  hacker x *cracker*, beyaz şapkalı x siyah şapkalı korsanlar

Siber Tehdit Temsilleri

Siber güvenlik politikaları kapsamında öne çıkan başlıca siber tehdit temsilleri:

- Siber Suçlar
- Siber Casusluk
- Siber Terörizm
- Siber Savaş

Siber Tehditler

Siber Suçlar (*cyber crimes*):

Bilişim sistemlerine **izinsiz girip zarar verme**

Bilişim sistemlerine **izinsiz girip** özel hayat ve haberleşme gizliliğini **ihlal etme**

Finansal suçlar

- Siber suçların özelliği bir **bilişim sistemi olmadan işlenememesi**dir. Yani bilişim sistemlerinin suça **özlü olarak** dahil olması lazım.
- İnternet aracılığıyla işlenen bütün suçlar siber suç **sayılmaz**. Bilişim yoluyla işlenen **asayiş suçları** da vardır (ör. internet aracılığıyla hakaret, tehdit) -> 5651 nolu yasa
- Çocuk pornografisi siber suç sayılmaktadır.
- Türkiye'de online kumar da siber suç sayılıyor

Siber Tehditler

Siber Casusluk (*cyber espionage*):

- Bilişim sistemlerinde **tutulan önemli, stratejik ve gizli bilgilerin** bilgisayar ağları üzerinden yetkisi olmayan kişi veya gruplarca **ele geçirilmesi.**
- **Devlet veya devlet-dışı aktörlerce devletlere veya ticari işletmelere karşı** gerçekleştirilebilir.
- Son örnekler: GhostNet (2009), Wikileaks (2010), Red October (2012), Snowden Vakası (2013), Sony Pictures (2014), Panama Belgeleri (2016), ABD seçimleri(2016), Macron'un seçim kampanyası (2017).

Siber Tehditler

Siber Terörizm

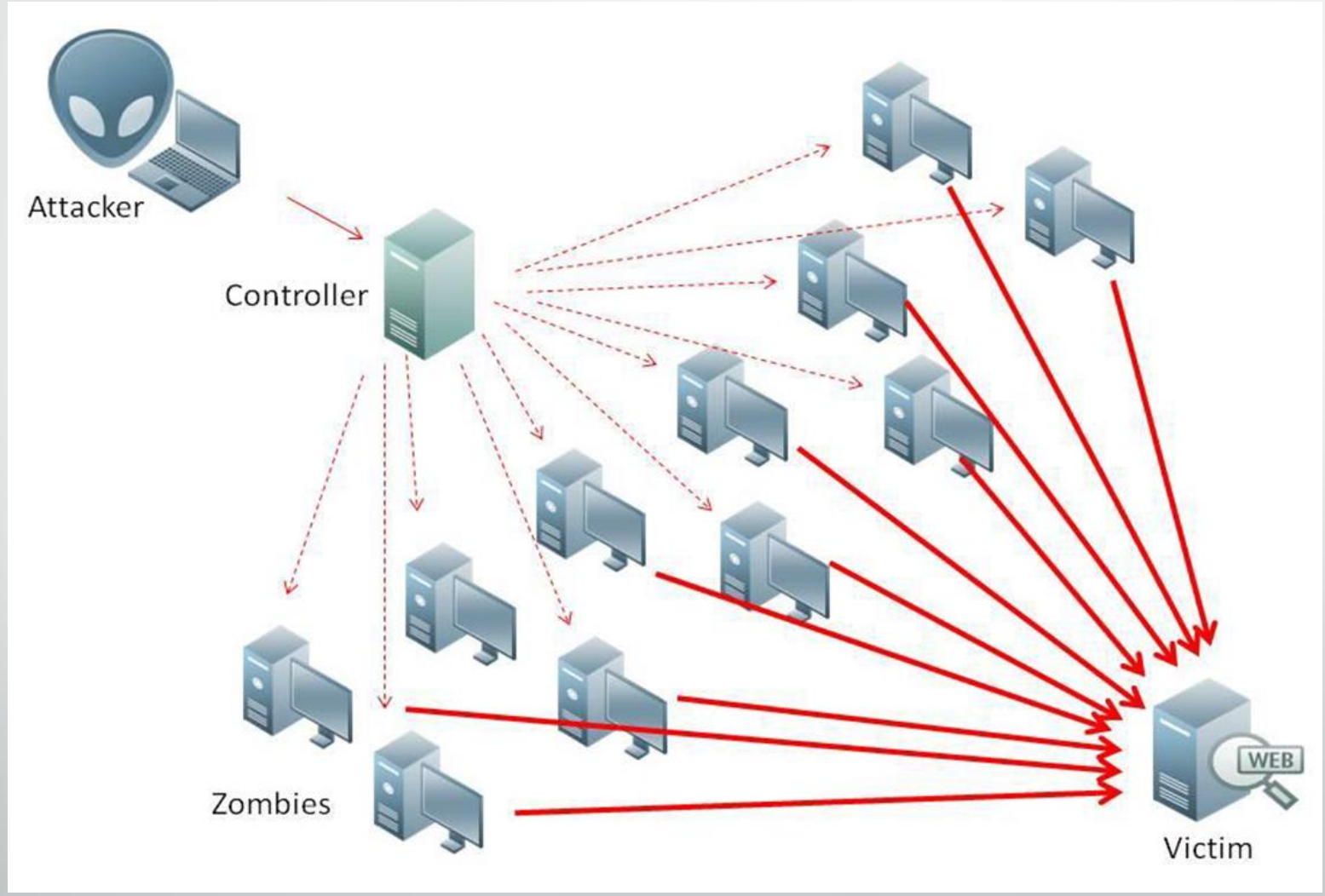
- Devlet dışı grupların bilişim sistemleri üzerinden kalkınmış ülkelerin kritik altyapı unsurlarına saldırarak ciddi fiziksel zarara yol açma ihtimali.
- Kritik altyapı unsurları (*critical infrastructure*), ulaşım, sağlık, su, enerji gibi sivil ve ekonomik hayat için vazgeçilmez altyapı unsurları.
- 1990'larda başta Batı ülkeleri olmak üzere tüm dünyada kritik altyapı hizmetleri bilişim sistemleri ve ağlarına bağlı otomasyon sistemlerinin kontrolüne girmeye başlıyor.
- Kötü senaryolar üzerinden ciddi bir güvensizlik kültürü besleniyor.
- Türkiye çapında 31 Mart 2015'te yaşanan elektrik kesintisinin sebebi siber saldırıydı

Siber Tehditler

Siber Savaşlar (/Çatışmalar):

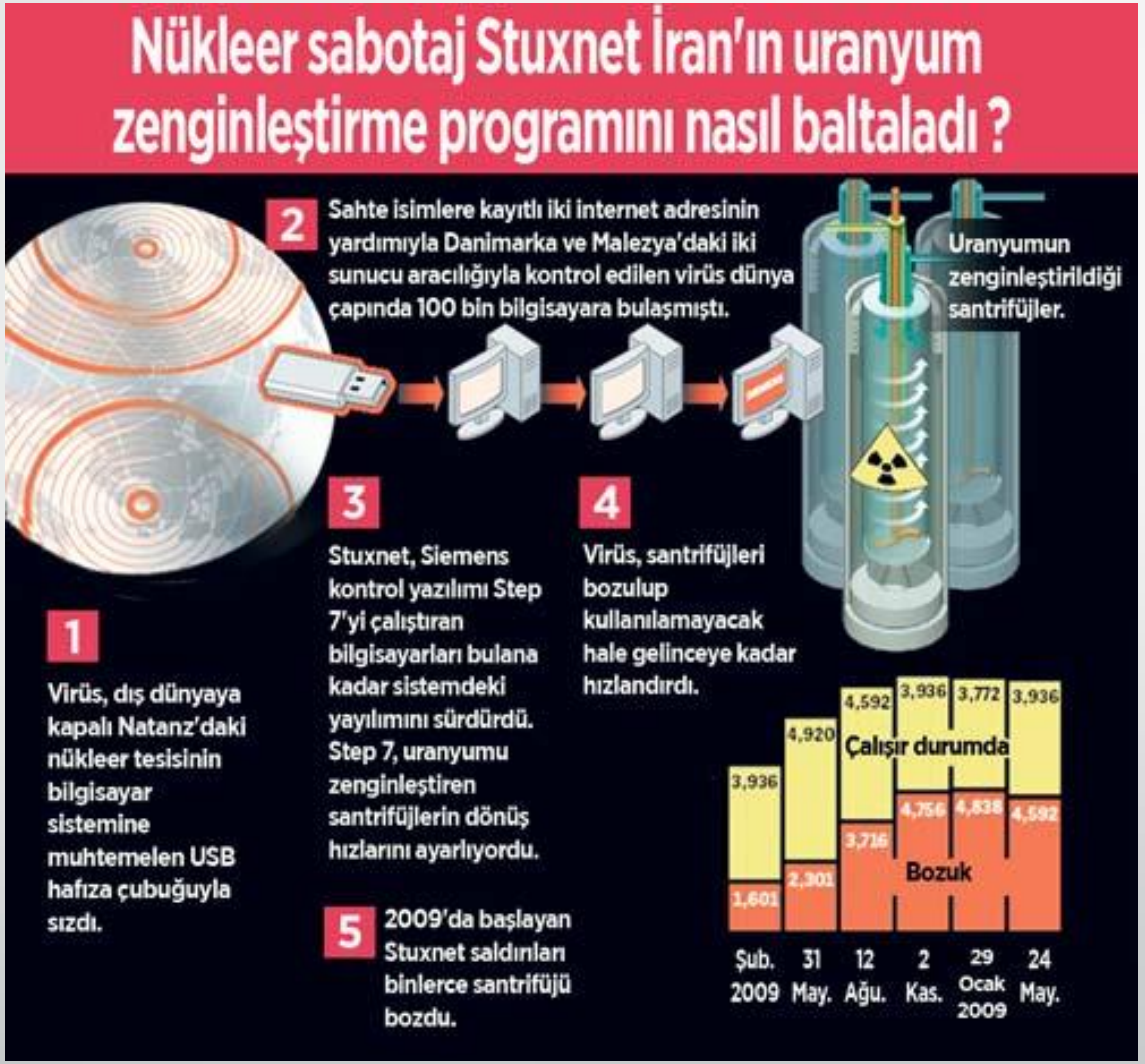
- Devletlerarası silahlı çatışmanın veya siyasi mücadelenin bir boyutu olarak, devlet-dışı aktörlerin de katılımıyla siber-uzayda gerçekleşen karşılıklı siber saldırı, propaganda ve dezenformasyona verilen addır.
- En tipik siber saldırı türü **DDoS**'tur (*Distributed Denial of Service*).
- Bunun dışında, siber saldırı olarak korsanlık ve casusluk faaliyetleri de yapılabilir. Devletlerin kritik altyapı unsurlarına zarar verilebilir (ör. stuxnet).
- Gelişmiş ülkeler bu tarz saldırılara daha açıktırlar.

DDoS Saldırısı



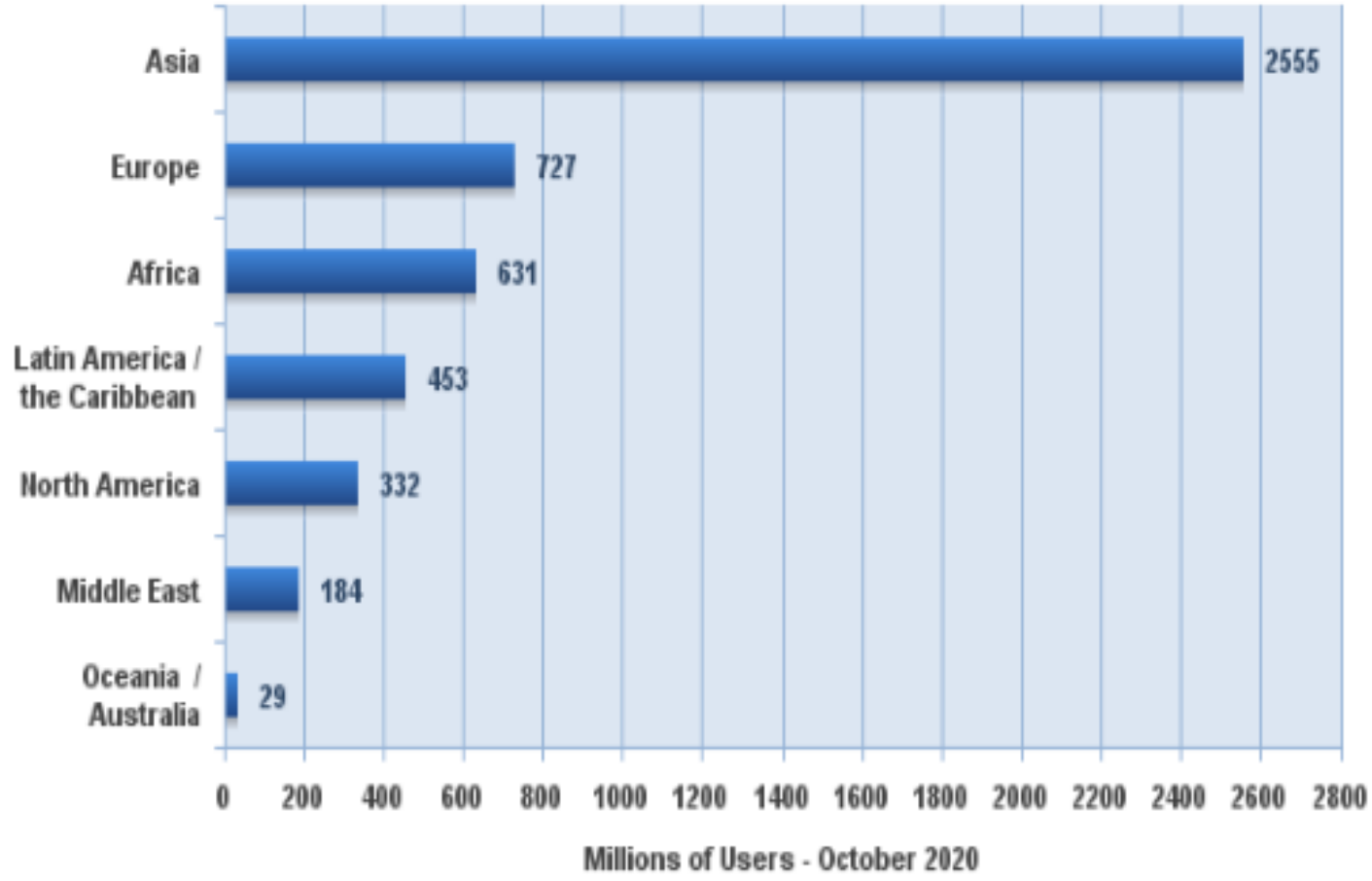
Şekil: https://media.scmagazineuk.com/images/2016/09/26/ddosattackex_1059804.png?format=png&zoom=1&quality=70&anchor=middlecenter&mode=pad

Stuxnet Saldırısı

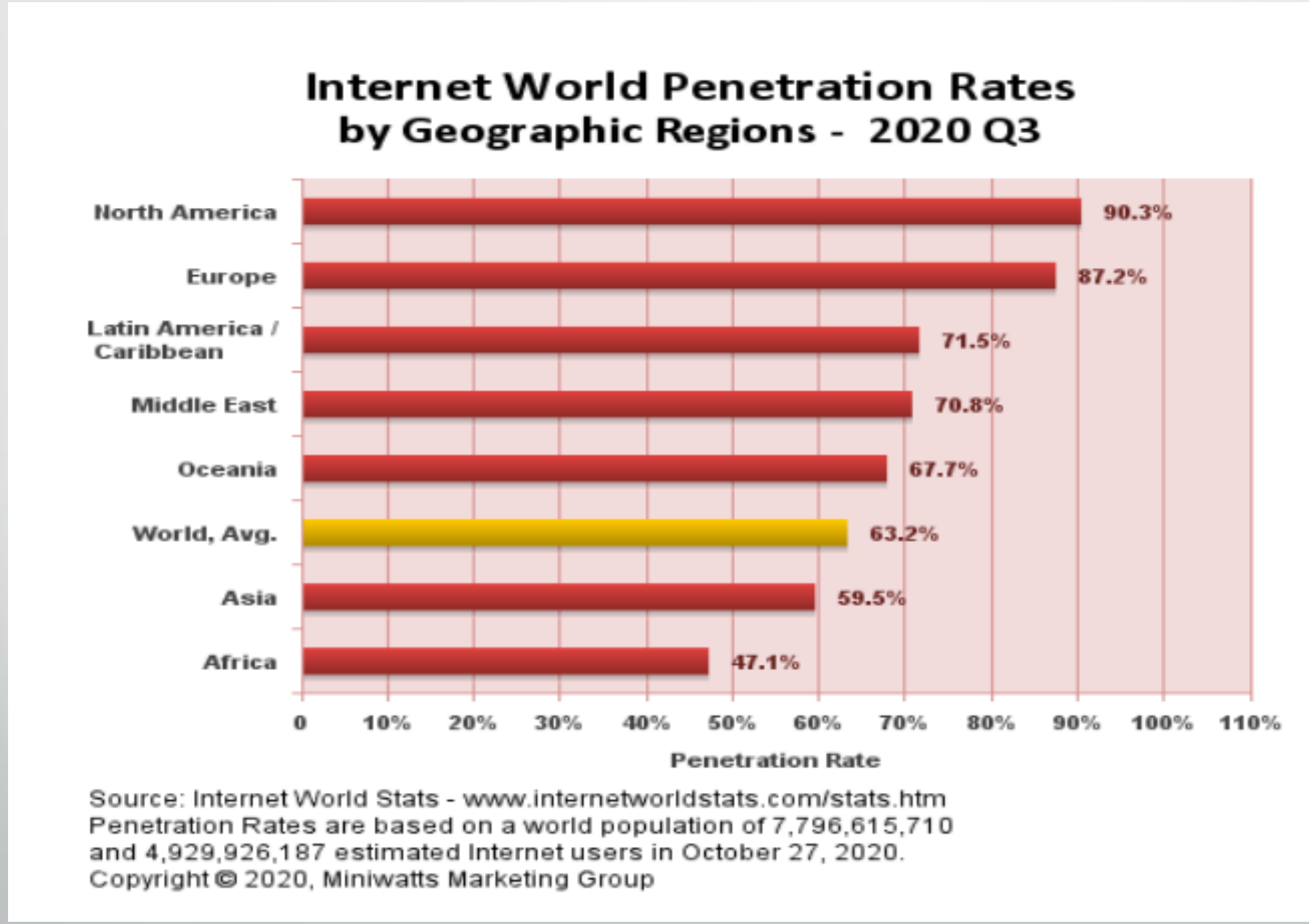


Şekil: http://i.milliyet.com.tr/GazeteHaberIciResim/2017/05/07/fft16_mf9075000.Jpeg

Internet Users in the World by Geographic Regions - 2020 Q3



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,929,926,187 Internet users estimated in October 27, 2020


Internet World Penetration Rates
by Geographic Regions - 2020 Q3
North America
Europe
Latin America / Caribbean
Middle East
Oceania
World, Avg.
Asia
Africa
90.3%
87.2%
71.5%
70.8%
67.7%
63.2%
59.5%
47.1%
0
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
110%
Penetration Rate
Source: Internet World Stats - www.internetworldstats.com/stats.htm
Penetration Rates are based on a world population of 7,796,615,710
and 4,929,926,187 estimated Internet users in October 27, 2020.
Copyright © 2020, Miniwatts Marketing Group

Siber Savaşlar

- **Siber savaş/çatışma örnekleri**: ABD-Çin (2001), ABD-Irak (2007), Rusya-Estonya (2007), Rusya-Gürcistan (2008), ABD/İsrail-İran (2010), ABD-Kuzey Kore (2011, 2014).
- Kuzey Kore (Büro 121), ABD (NSA)
- Siber Uzay, gerek devletler arasındaki, gerekse devletler ile devlet dışı aktörler arasındaki güç asimetrisini ortadan kaldırma potansiyeline sahip.
- hacker + activism -> *hacktivism* -> ör. Anonymous, Redhack
- Siber aktivizm de giderek güvenlikleştiriliyor.

Siber Güvenlik Politikaları

- ABD: International Strategy for Cyber Space (2011) -> siber saldırı bir savaş nedeni sayılıyor, DoD Strategy for Operating in Cyber Space (2011), DoD Cyber Strategy (2015).
- NATO: NATO Siber Savunma Yönetimi Otoritesi (2008)
- AB: Dijital Gündem (2010), Siber Güvenlik Stratejisi (2013)
- Türkiye: Siber Güvenlik Kurulu (2012), Siber Güvenlik Siyaset Belgesi (2013), Ulusal Siber Olaylara Müdahale Merkezi (2014).

Siber Güvenlik Politikaları

- Siber uzayın saldırıyı kolaylaştıran yapısı.
- Mutlak güvenliğin imkansızlığı -> risk yönetimi -> direnç ve esneklik (*resilience*)
- Kamu-özel sektör ortaklığı -> dağıtılmış sorumluluk
- Siber caydırıcılık -> ne kadar mükün?
- Abartılı bir tehdit ve risk söylemiyle güvensizlik kültürü besleniyor