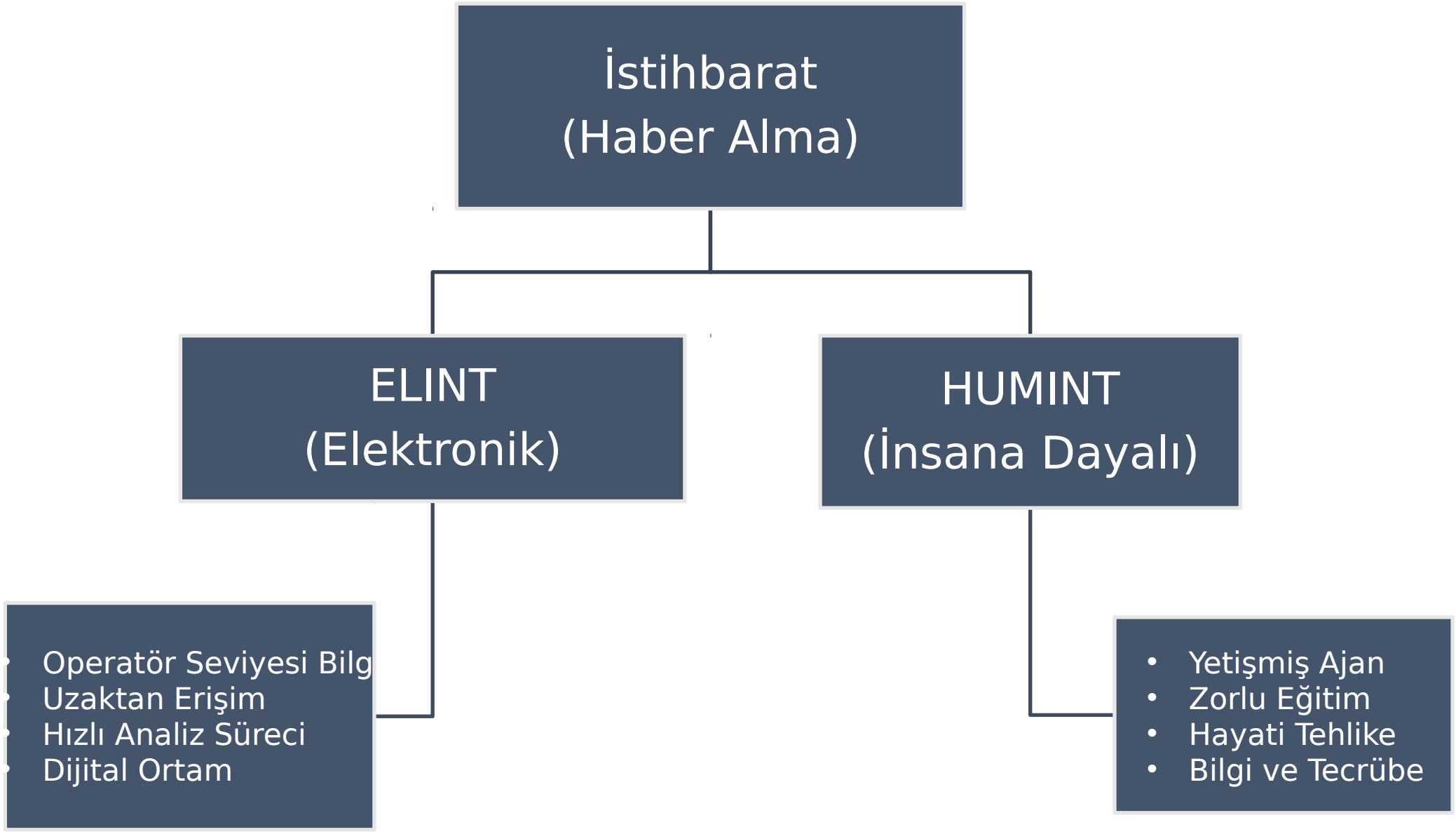
Tempest Sinyal İstihbaratı

Hasan BASKIN

2020
SAKARYA


İstihbarat
(Haber Alma)
ELINT
(Elektronik)
HUMINT
(İnsana Dayalı)
Operatör Seviyesi Bilg
Uzaktan Erişim
Hızlı Analiz Süreci
Dijital Ortam
Yetişmiş Ajan
Zorlu Eğitim
Hayati Tehlike
Bilgi ve Tecrübe

Tempest Nedir ?

- «Transient Elektromagnetic Pulse Emanation Standard»
- Elektromanyetik sinyal yayan elektronik cihazların güvenliğinin sağlanması için geliştirilmiş bir **standarttır.**
- **Gizlilik dereceli bilgi** işleyen elektriksel veya elektronik cihazlardan kaynaklanan **istenmeyen elektromanyetik enerji yayılımları** ile bu yayılımların araştırılması, incelenmesi ve denetim altına alınması olarak tanımlanır.
- Elektronik cihazların bulunduğu ortamlarda temelde **2 durum** söz konusudur.

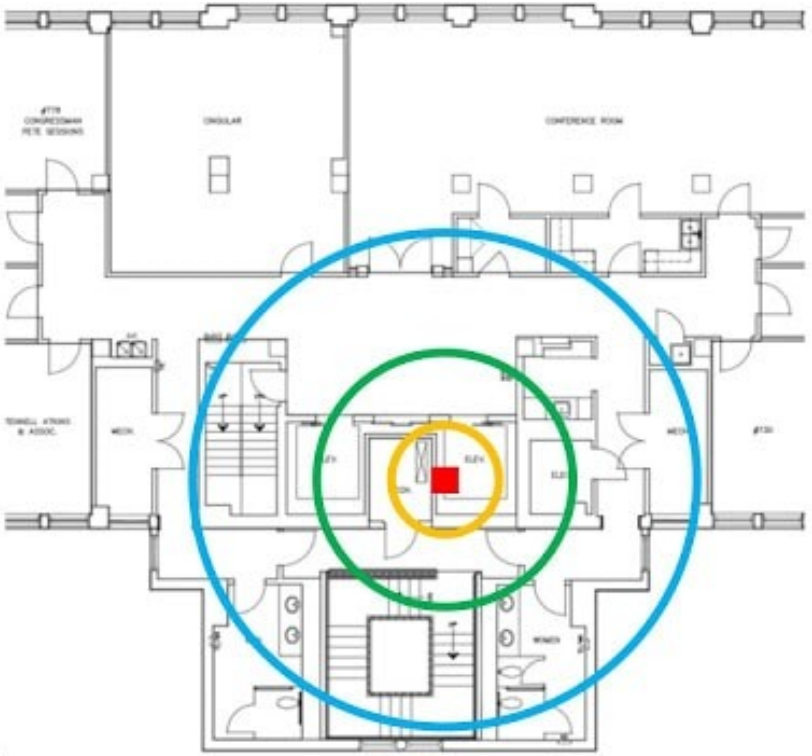
Elektromanyetik Girişim (EMI)

- Elektronik bir cihazdan ortama yayılan elektromanyetik dalgalar nedeniyle ortamdaki cihazlar üzerinde meydana gelen bozulma veya kötüleşme durumu.

Elektromanyetik Uyumluluk (EMC)

- Birden fazla elektronik cihazın aynı ortamda yayılan elektronik dalgalardan etkilenmeden uyum içerisinde çalışması devam etmesidir.

- Elektronik dalgalar ortam ve cihaz özelliklerine göre **800 ile 1600** metre arasında yayılabilir.



Bazı Tempest Terimleri

Kırmızı

- Başkaları tarafından **ele geçirilmesinin istenmediği** bilgilerin bulunduğu bir bilgisayar ağının bütün bileşenleri.
- Kriptolanmamış **gizli bilgiyi taşıyan** kablolar, optik fiberler, elemanlar, cihazlar ve sistemler.

Siyah

- Hiç bir kırmızı sistemin bulunmadığı bir bölgedir.
- **İnternete bağlanan** herhangi bir bilgisayar.
- Gizli işaretlerin bulunmadığı kablolar, optik fiberler ve elemanlar
- **Gizli bilgi saklanmamalıdır.**

Tempest ile Gelen Riskler

- Özel Hayatın İfşa Edilmesi
- Ülkeler Arası Kaos Ortamının Oluşması
- Gizli Bilgilerin/Verilerin (Ulusal veya Bireysel) İfşa Edilmesi
- Kişisel Verilerin Çalınması
- Haberleşmenin Manipüle Edilmesi
- Elektrik ve İletişim Ağının Zarar Görmesi
- Milli Kripto Algoritmalarının Deşifre Olması
- Savaş ve Savunma Stratejilerinin Ortaya Çıkması

Bilgi İçeren Kaçaklar

- Ele geçirilip incelendiğinde iletilen, alınan veya saklanan herhangi **bir veri ile ilgili** kaçak **elektromanyetik işaretlerdir**.

İletkenden Arındırılmış Bölge

Kırmızı cihazın etrafında hiçbir siyah iletken veya cihaz olmaması gereken bölge.

- Dış dünyadan **yalıtılmış** alan.
- Bu bölgede **bilgi kaçağı** olma olasılığı çok yüksektir.
- Bölgenin büyüklüğü kullanılan cihaza göre değişir.

Tempest Kaçakları

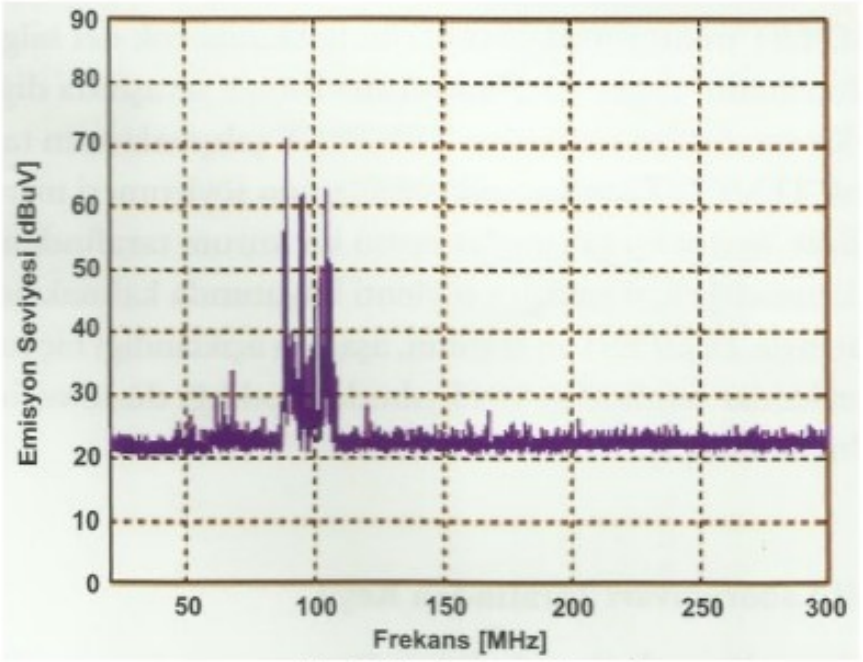
- Bu kaçaklar istem dışı oluşmaktadır. (İstemli RF Yayını Değildir !)
- Belli frekanslarda bilgi taşıyan işaretlerdir.
- Havadan veya kablo üzerinden yayılırlar. **ANTEN** kullanılarak havadan veya **PROB** kullanılarak kablodan elde edilebilir.
- Ele geçirildiğinde anlamlı görülmeyebilir, **çözümlenmesi** gerekir.
- Çözümlemeler sonucu elde edilen bilgiler şifrelenen açık bilgileri içerir.
- Bunların en genel olanları; **temel bant kaçakları**, **genlik modülasyonlu (AM) kaçaklar** ve **darbe kaçaklarıdır**

Bilgi İçeren Kaçakların Oluşumu

Bu noktada sayısal devrelerdeki işaret oluşum aşamalarının incelenmesi gerekir.

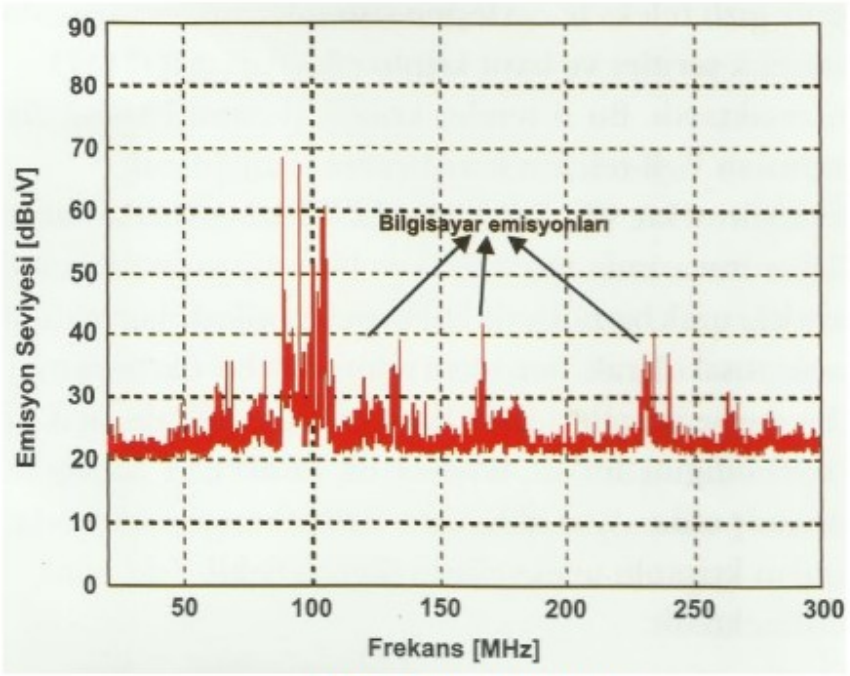
- Sayısal devrelerde işaretler **0 ve 1** lerden oluşur.
- 0 Seviyesinden 1 seviyesine geçerken tüketilen enerji, 1 seviyesinde kalmak için tüketilen enerjinin **1000 katıdır.**
- Oluşan Enerji Açığının;
  - %1: Yeni Gerilim Seviyesinin Sürdürülmesi
  - %4: Isı
  - **%95 :** Elektromanyetik dalga olarak ortama yayılır. **(Gürültü yada Gizli Bilgi)**

Bilgisayar Emisyonlarının Spektrumda Gösterilmesi



(a) Bilgisayar Kapalı

80-110 Mhz. Aralığındaki FM Radyo Frekansları

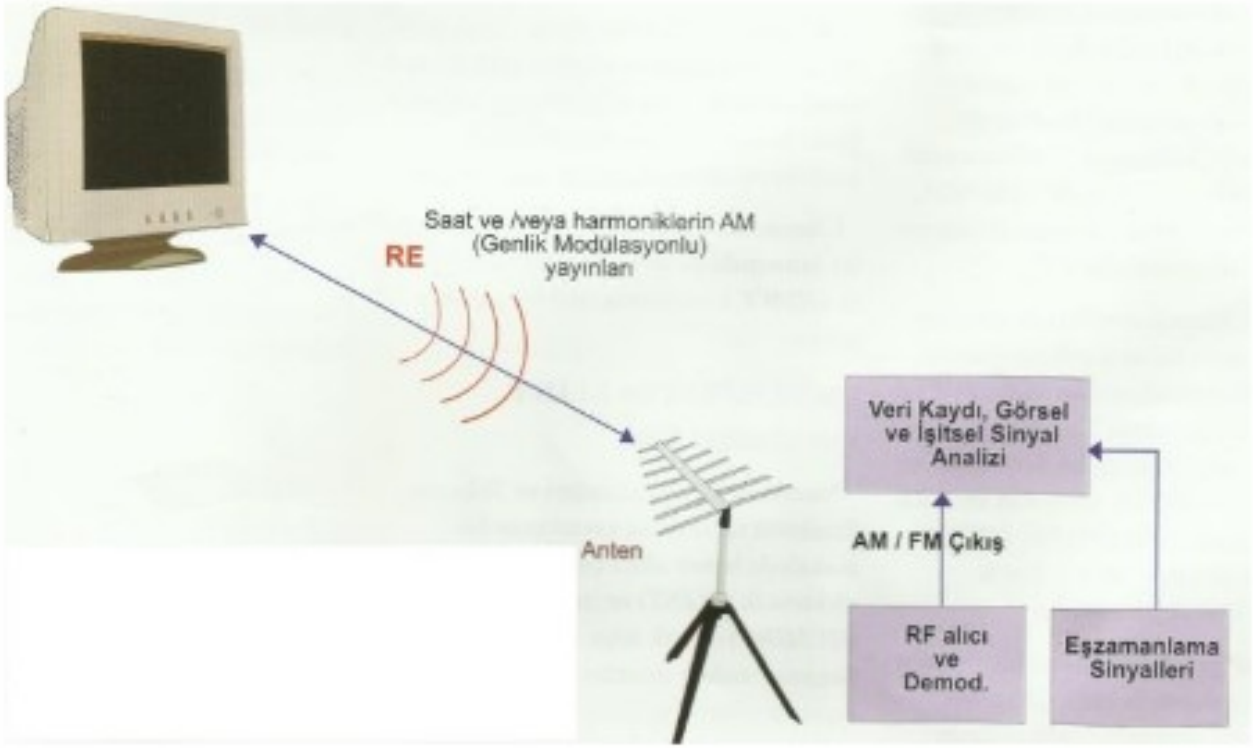


(b) Bilgisayar Açık

Farklı frekansta yayılımlar başladı.

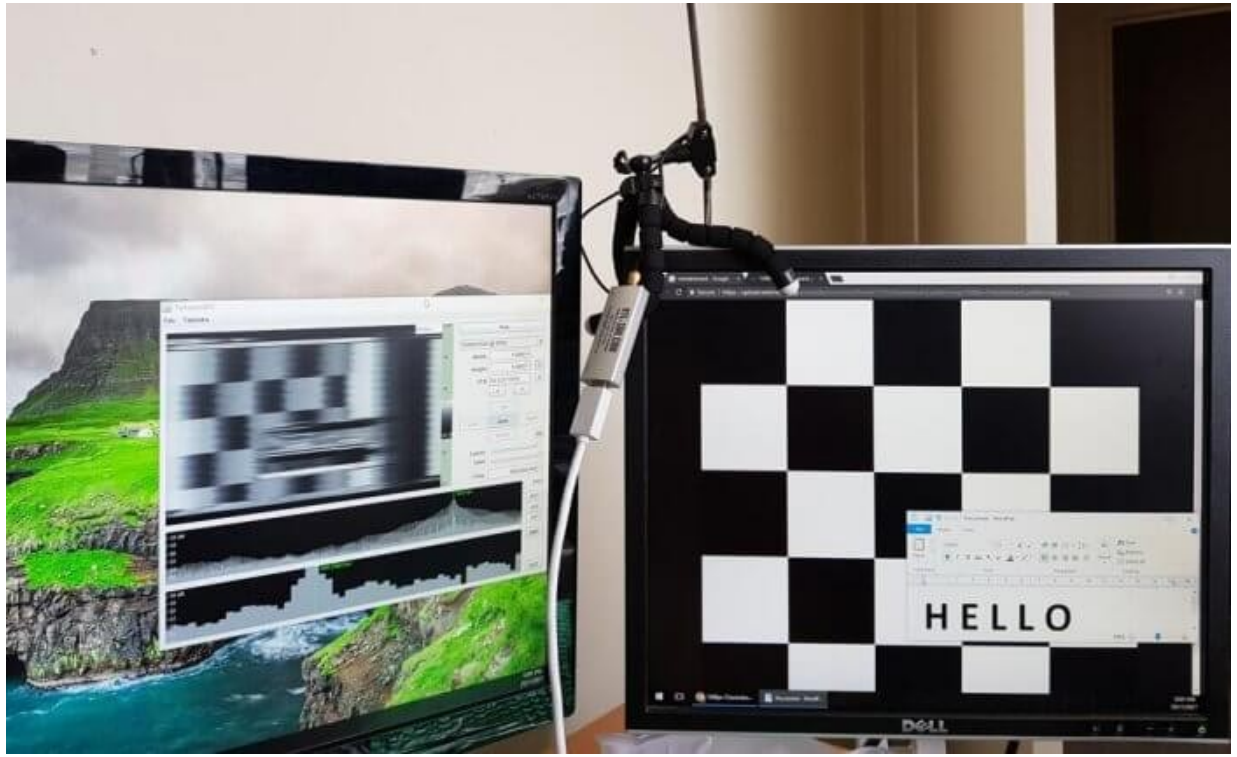
Van Eck Düzeneği

- Hollandalı Araştırmacı **Van Eck**, **1985 yılında** bilgisayar ekranlarından yayılan emisyonları işleyerek **orijinal görüntüyü** elde etmeyi başarmıştır.
- Böylece kamuoyuna ilk kez **TEMPEST** kavramı duyrulmuştur.



Bilgisayar Ekran Kaçakları

- **HackRF One**
- **RTL-SDR**



Elektromanyetik Güvenlik

- Tempesti de içine alan genel bir kavramdır.
- Gizli bilgi işleyen cihazlardan **elektromanyetik olarak sızan** bütün bilgilerin **güvenliğini** ifade eder.
- **TEMPEST**, **NONSTOP**, **HIJACK** saldırılarının önlenmesi.

NONSTOP

Gizli bilgi işleyen bir cihazın yakınındaki **RF vericiler** üzerinden gizli bilginin yayınlanmasıdır. Bu cihazlar;

- Cep telefonu
- Telsiz
- Radar
- Kablosuz Klavye
- Kablosuz modem
- Kablosuz alarm sistemi

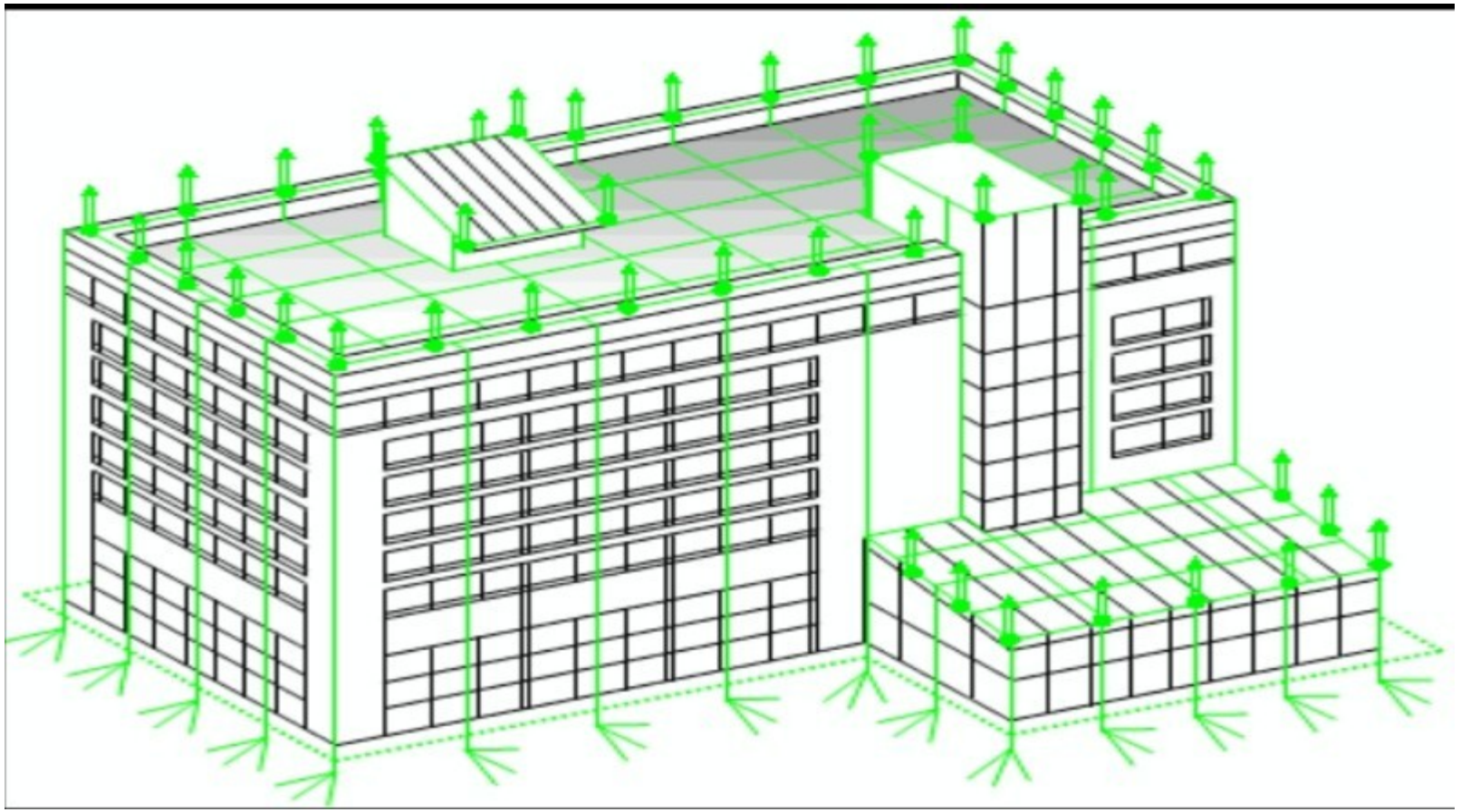
HIJACK

İşlenen gizli bilgilerin kriptolanmış ve dış ortama **açık hatlar** üzerinden yayınlanmasıdır.

Tempest Önlemleri

- İlk olarak gizli bilginin istenmeyen bölgelere **hangi yollarla** ulaştığının tespit edilmesi.
  - **Uzaysal Işıma** (Havaya yayılan enerji yolu.)
  - **Elektriksel İletkenlik** (Kablolar, kalorifer tesisatı vb. metal eleman yoluyla.)
- Kırmızı ve siyah kabloların **izole** edilmesi
- Cihazların **test** edilmesi ve **uygun bölge**lerde kullanılması
- **Doğru tipte kablo** kullanımı ve **Doğru Tesisat**
  - (Shielded CAT6 yada CAT7 & Fiber Optik)
- Uygun **güç ve işaret hattı filtrelemesi** yapmak
- Gizli bilgi işlenen bölgelerin elektromanyetik olarak **izole** edilmesi

Bina Yalıtımı ve Topraklama



Faraday Kafesi – İzole Ortam

Kaynaklar

- http://www.erikyyy.de/tempest/
- https://www.rtl-sdr.com/tempestsdr-a-sdr-tool-for-eavesdropping-on-computer-screens-via-unintentionally-radiated-rf/
- https://dergipark.org.tr/tr/download/article-file/768686, https://ab.org.tr/ab13/bildiri/129.pdf
- https://www.resmigazete.gov.tr/eskiler/2019/07/20190706-10.pdf