Yazarın bu bölümdeki diğer yazıları...

- Siber Savaşta Yeni Cephe: İRAN-Buşehr Nükleer Santrali ve SCADA-PLC Sistemler
- Siber Savunma için Karar Destek Sistemi ve İstihbarat Stratejisi
- Mimari Yapılarda, Bilgi Güvenliği Tasarım ve Uygulamaları, SağırOda
- Ağ Merkezli Savaşta, Aviyonik Sistemleri Bulandırma Saldırıları
- Savaş Cephesi Olarak, Sanal Ortamda Savunma ve Saldırı
- Bilgi Teknolojileri Kapsamında, Kurumlarda Sanayi Casusluğunu Nasıl Önleriz?
- Ulusal Güvenliğin Zayıf Halkası E-devlet

Adli Bilişim Kapsamında, Sahte Dijital Belgelerle Savaş ve İşgalin Değerlendirilmesi.

Cenk Ceylan, Turkish Forensic / GÖKTÜRK BT Ltd. 10.06.2011

*Irak'ta nükleer silah geliştirme amacıyla, Saddam Hüseyin yönetiminin Birleşmiş Milletler engeline rağmen, Afrika-Nijer'den toz halinde Uranyum almak istediği, İtalyan İstihbarat kuruluşu (SISMI) yöneticisi olan Nicolò Pollari tarafından**, Amerikan dış (merkezi) istihbarat kuruluşu, (CIA) üst yönetimine, yapılan bilgilendirme "**Irak: Nükleer teknolojiyle ilgili tedarik çabaları" **toplantısında CIA-Roma temsilcisi tarafından 18 Ekim 2001 tarihinde, ilk dijital belge olarak iletilir.***

- *10 Mayıs 2002: CIA Yakındoğu ve Güney Asya Analiz Departmanı (NESA) hazırladığı brifingde Irak'ın kitle imha silahı programına dair bilgileri yeni belgeye göre güncellemiştir. Yazılanlarda yabancı bir devlet gizli servisine göre Irak'ın Nijer'den 500 ton uranyum almaya çalıştığı belirtilmektedir.*
- *22 Temmuz 2002: ABD Enerji Bakanlığı tarafından hazırlanan raporda Irak-Nijer uranyum anlaşmasına dair istihbarat bilgisine göre Irak'ın nükleer silahlanma programını yeniden başlatmakta olabileceği belirtilir.*
- *9 Eylül 2002: SISMI'nin o dönemdeki başı Nicolò Pollari, gizlice Washington'a gelerek Beyaz Saray'ı doğrudan bilgilendirip, dönemin ABD Ulusal Güvenlik danışman yardımcısı Stephen Hadley ile görüşür. Bundan sonra,Irak'ın Nijer'den uranyum aldığına dair savlar giderek güçlenir. Bu bilgi üzerine ABD hükümeti Başkan Bush'un 12 Eylül 2002 günü Birleşmiş Milletler Genel Kurulunda yapacağı konuşmaya bu konuyu da eklemeyi planlar. Ancak CIA yetkilileri konuşma metnine müdahale ederek konuşmanın yapılmasına 24 saat kala bu konuyu konuşma metninden çıkartır. Bu bilgi, Birleşik Krallık, dış istihbarat kurumu (MI6) raporu olan Beyaz Kitap'da yer alır.*
- *ABD Başkanı Bush 29 Ocak 2003'deki ulusa sesleniş konuşmasında dile getirdiği, "Saddam Hüseyin'in nükleer silah üretme çabaları", Mart ayında başlatılacak Irak'ın işgali için en önemli gerekçelerden birisini oluşturacaktır.*

İtalyan istihbaratına dayandırılan savlar, Irak Savaşı öncesinde ülkeye silahlı müdahaleyi savunan ABD ve İngiltere tarafından sorgulanmadan sahiplenilmiş ve ABD Başkanı George W. Bush tarafından, 29 Ocak 2003 tarihinde yapılan ulusa sesleniş konuşmasında kullanılmıştır."The British government has learned that Saddam Hussein recently sought significant quantities of uranium from Africa" "*İngiliz Hükümeti, Saddam Hüseyin'in yakın bir zamanda Afrika'dan önemli bir miktarda uranyum tedarik etmeye çalıştığını öğrenmiş bulunuyor."*

Belgelerden haberdar olan Fransız istihbaratı Bush'un konuşmasından bir yıl önce ABD yönetiminin uyararak savlara dair hiçbir kanıt bulunmadığını bildirmiştir.

*Irak Savaşı'nın başlamasından önce 2003 yılı başında Uluslararası Atom Enerjisi Kurumu başkanı **savlarla ilgili yaptığı açıklamada dijital belgelerin sahte olduğunu açıklar**. Ajansın başkanı Muhammed El Baradey vardıkları bu sonucu Birleşmiş Milletler Güvenlik Konseyine de açıklamıştır.*

İtalyan İstihbarat Kuruluşu (SISMI) bünyesinde 2005 yılında yapılan soruşturma sonucunda, uluslararası etkileri büyük olacak bir skandal ortaya çıkartılır. Irak yönetiminin Nijer'den uranyum tozları aldığına dair sahte dijital belgelerin, kuruluştaki albay Antonio Nucera tarafından üretildiği anlaşılmıştır!

2000 yılında, İbrahim El Maraşi, Harvard Üniversitesinde doktora öğrencisiyken, **Saddam Hüseyin'in iktidarını ayakta tutan korku sistemini inceleyen tez** çalışmasını yarıda bıraktıktan sonra, bir bir derginin isteği üzerine makale hazırlar ve Eylül 2002 de internette yayınlanır.

Birleşik Krallık-Britanya başbakanı Tony Blair ve Amerikan Dış İşleri bakanı Colin Powell tarafından 5 Şubat 2003 tarihinde, Birleşmiş Milletler Güvenlik Konseyi'ne kanıt olarak sunulan dijital (Word) belgede (İngiliz istihbarat raporu), Irak'ta kitle imha silahları olduğuna dair bir rapor yer alır.

Tony Blair tarafından, Birleşmiş Milletler Güvenlik Konseyine kanıt olarak sunulan raporda, Cambrigde üniversitesinden Dr. Glen Rangwala tarafından, bazı çalıntı ifadeler olduğu tespit edilir ve İbrahim El Maraşi'ye daha önce hazırlanan makalesinden bire bir çalınan ifadeler ve yeni-farklı ilavelerin olduğu haberi verilir.

Ağustos 2003 tarihinde, AT&T laboratuvarın da çalışan Simon Byers isimli bilgi güvenliği ve adli bilişim araştırmacısı, Tony Blair'in sunduğu Word belgesini internetten indirerek, üzerinde daha önce yapılan değişiklikleri ve gizli bilgileri tespit etmek için adli bilişim uygulamalarıyla bir dizi inceleme yapar.

Rev. #1: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #2: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #3: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq – security.asd"
Rev. #4: "JPratt" edited file "C:\TEMP\Iraq - security.doc"
Rev. #5: "JPratt" edited file "A:\Iraq - security.doc"
Rev. #6: "ablackshaw" edited file "C:\ABlackshaw\Iraq - security.doc"
Rev. #7: "ablackshaw" edited file "C:\ABlackshaw\A;Iraq - security.doc"
Rev. #8: "ablackshaw" edited file "A:\Iraq - security.doc"
Rev. #9: "MKhan" edited file "C:\TEMP\Iraq - security.doc"
Rev. #10: "MKhan" edited file "C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc"

Sonuçlar çok şaşırtıcıdır. Dijital belgenin meta verileri için de yer alan ve asıl yazıldığı kaynağa ilişkin, referans bilgiler bir savaşın kaderini değiştirecek nitelikteydi. Birleşmiş Milletlere sunulan raporun, (dijital belge-Word) **tam 10 defa değiştirilerek kayıt edildiğini tespit eder.**

İbrahim El Maraşi kendisiyle Hürriyet gazetesinde Gaye Güzelay tarafından yapılan mülakatta şunları ifade eder. Rapor İngiltere'de Parlamento'ya sunulmuş, milletvekilleri Irak'a karşı savaş kararını bu istihbarata dayanarak desteklemiş. Tony Blair o kadar beğenmiş ki raporu, o zamanki Amerikan Dışişleri Bakanı Colin Powell'a vermiş. O da BM Güvenlik Konseyi'ne 5 Şubat 2003'te sundu bu raporu. Savaşa girilmesiyle ilgili önemli konuşmasında "Bu istihbarat raporuna bakın, benim savımı doğruluyor" dedi.

Ben de Powell'ı televizyondan seyrediyordum o sırada. Cambridge'deki profesör (Dr. Glen Rangwala), çevresine bu raporun bir kısmının benim makalemden çalındığı yolunda mail gönderiyormuş. Bir sabah uyandım, resmim ve ismim gazetelerdeydi! O sırada bir araştırma merkezinde çalışıyordum. Sabah işe gittim, mail kutumu açtım, röportaj için 300 mail gelmişti. Telefonum devamlı çalıyordu. 24 saat boyunca devamlı röportaj veriyordum. Bu arada İngiltere ve Amerika savaşa girmeye karar vermişti. Google'da 60 hitim olduğu için çok mutlu olduğumu söylemiştim ya, bu olaydan sonra 600 bine çıktı. Irak savaşı başladı. **Toplu imha silahları bulunamadı. İnanılmaz casus ağına sahip, dünyanın en büyük kuvveti benden makale çalmış ve sadece tahminlerle savaşa girmişti"**

İstihbarat raporunun 9 sayfası benim makalemden alınmaydı. Profesöre yanıt yazdım, istihbarat raporuyla hiçbir ilgim olmadığını, internetten makaleyi indirmiş olabileceklerini söyledim. Çünkü rapordaki noktalama işareti yanlışları bile aynıydı. En önemlisi, makalemde yazılan hiçbir şey, İngiliz veya Amerikalıların savaşa girmelerini destekleyici nitelikte değildi. Toplu imha silahlarıyla ilgili hiçbir şey makalemde yer almıyordu. Sadece Irak'taki polis devletiyle ilgili kısımda benim makalem kullanılmıştı. **Raporun ikinci bölümünde, Saddam'ın gizli örgütleri kullanarak toplu imha silahlarını sakladığı söyleniyordu, bunun benim makalemle hiç ilgisi yoktu**. Okuyucular ikisi arasındaki farkı anlamadı. " İbrahim El Maraşi Türk üniversitelerinden, Sabancı ve Koç üniversitelerinde hoca olarak bir dönem çalıştı.

2010 yılında, A.B.D-Washington da yapılan, dünyanın en önemli bilgi güvenliği ve hacker konferansı, Blackhat ' de, Symantec şirketinden **Qing Wang** tarafından yapılan "**MS Office War**: **Parse deeply, fuzz widely, shoot precisely and measure scientifically**" sunumda, dijital ofis belgeleri, Word, Excel, Powerpoint, nasıl bulandırılacağı yazan-kaydeden bilgilerinin nasıl değiştirilebileceği adli bilişim yöntemleriyle anlatılıyor ve bu konuda **Megatron** adıyla bir bulandırma yazılımı tanıtılıyordu.

Tesadüfen aynı tarihlerde, Türkiye de hükümeti yıkmaya ve darbe yapmaya yönelik planların olduğu savıyla, gündemi sarsacak dijital ofis belgelerini delil olarak kabul eden mahkemelerce, **Türk Silahlı Kuvvetleri** üst yönetiminde görevli kişiler sanık olarak, **Balyoz, Suga, Kafes** vb. davalarında yargılanmaya başladılar. **Dijital belgelerin**, Emniyet Genel Müdürlüğü, Adli Bilişim Laboratuvarları ve TÜBİTAK incelemeleri sonucunda hazırlanan adli bilişim analizi raporlarının hiç birisinde, dijital ofis belgelerinin bulandırılabileceği ve sahte olabileceklerine dair bir bulgu, emare yer almıyordu.

Yakın zamanda, Askeri Casusluk savsıyla açılan davada, savunma avukatların aynı marka ve seri numaralı, taşınabilir veri depolama delilleri Sandisk ve Kingston marka USB belleklerin bir başka dava olan Poyrazköy'de yer aldığına ilişkin savları, **Emniyet Genel Müdürlüğü basın açıklamasıyla** (USB bellekler aynı seri numaralı olabilir) ve mahkemeye getirilen diğer dava delilleriyle karşılaştırılarak aynı olduğu görüldü şeklindeki mahkemenin açıklamaları, adli bilişim için tam bir bilimsel yanlışı beraberinde getiriyordu.

Oysa ki, dünya üzerinde üreticiler, hiç bir veri depolama cihazı ,sabit diskler, USB bellekler için aynı seri sayısı (numarayı) kullanmazdı, kullanamazdı.

Aksi halde, bilişim sanayi için her üreticiye, suça ilişkin delilleri elektronik olarak takip için arka kapılar bırakması için direktifler veren, klavye üretimine dahi müdahalede eden, Amerikan Ulusal Güvenlik kurumu, NSA boşa uğraşmış olurdu.

Aynı marka ve model USB belleklerin, aynı seri numarasına sahip olduğu ve çok sayıda üretildiği gibi, talihsiz açıklamayı yapan EGM yöneticileri, bunun böyle olmadığını deneyerek görebilirler. Bunun ispatı için, aynı marka ve model USB bellekler, adli bilişim analizi ve imaj alma yazılımları, (Guymager, Encase, FTK vb.) incelenebilir ve farklı seri sayılı (numaralı) olduğu görülür.

Dijital delillerin en temel özelliği, tıpkı fiziksel deliller gibi, benzersiz, inkar edilemez ve bütünlüğü doğrulanabilen nesneler olmasıdır. Aksi halde, aynı USB bellekleri adli bilişim analiz için alınan imajlarındaki seri sayısından ayırmamız mümkün olmazdı.

Aynı marka ve model USB belleği fiziksel olarak birbirlerine benziyorlar diye ve sırtlarında aynı model sayısı (numarası) yazıyor diye, aynı seri sayılı (numaralı) olarak tutanaklara ve elektronik imaj alma dijital belgesine yazmak, eğer kasıt yoksa delillerin toplanması, sınıflandırılması ve karşılaştırılması - karıştırılması konusunda çok vahim bir adli bilişim yetkinsizliğidir.

Bu durumda mevcut davalar için dijital belgelerin yer aldığı, elektronik delillerin adli bilişim analiziyle incelenmesi sürecine bilimsel olarak gölge düşmektedir.

Geçen hafta, Avrupa seyahatinde bulunan A.B.D başkanı Barack Hüseyin Obama, Kongre'nin süresini uzattığı terörle mücadele önlemlerini içeren terör yasasını, **imza makinesiyle onaylayınca** ülkede '**ıslak imza**' tartışması başladı.Yasa için ıslak imza robotu kullandığı ve bu konunun ahlakı olarak ileride, hastayken kötü niyetli olarak kullanılabileceği ülkede tartışılmaya başlandı. Konu hakkında, NewYork Times, 28 Mayıs 2011 tarihinde, Michael D. Shear bir makale yazdı.

Tesadüfen yine aynı tarihlerde Türkiye'de, aynı davalar için ıslak imzalı olarak bulunduğu sav edilen fiziksel kağıt belgelerdeki imzaların, savunma avukatları tarafından, geçmişte makine (autopen) ile taklit edilerek oluşturulduğu sav edilmişti. Tüm bu ifadeler, ıslak imza delillerinin incelenmesi için adli bilişime yeni bilimsel tartışmalar kazandıracak. Tübitak tarafından imza incelemek için yapılan, farklı dalga boylarındaki ışığı yansıtarak, imza değişikliği vb. tespite yarayan renk temelli bilimsel patentli yöntem, aynı imzayı atan ıslak imza robotu (autopen) ve benzerlerini ayıran grafoloji bilimi karışımıyla yeni analizler için önemli hale gelecek.

Bu süreçte adli bilişim analizi için en hassas konu, delillerin bilimsel olarak toplanması, sınıflandırılması, uzmanlarca özel sektöre de açık olarak incelenmesi, olay örgüsünün keşfi için incelemenin delil havuzuyla karşılaştırılmalı (USB-bilgisayar-DVD-ROM-DVD yazcı vb) olarak bilimsel şekilde siyasi kaygılardan uzak yapılması, gelecekte oluşabilecek hak ihlallerini önlemek için çok önemlidir!

Sonuç, önemli davalar, savaşlar ve işgal planları için sunulan dijital belgelerin (word-Excel-PowerPoint-Acrobat), bulandırılıp, üst veri yolları, tarihi, yazan, kaydeden vb. dosya öz niteliklerinin değiştirilebildiği, sahte çıkabileceği unutulmamalıdır!

Kaynakça:

G. Bush'un konuşması,
http://en.wikisource.org/wiki/George_W._Bush%27s_Third_State_of_the_Union_Address

Nijerde Uranyum satışı makalesi; Los Angeles Times,
http://pqasb.pqarchiver.com/latimes/access/988523441.html?dids=988523441:988523441&FMT=ABS&FMTS=ABS:FT&type=current&date=Feb+17%2C+2006&author=Bob+Drogin+And+Tom+Hamburger&pub=[HOME+EDITION]%3B+Los+Angeles+Times&edition=&startpage=A.1&desc=The+Nation

Tony Blair'in sahte raporu
http://www.computerbytesman.com/privacy/blair.htm
http://www.hurriyet.com.tr/pazar/5138238.asp
http://www.antionline.com/showthread.php?t=253289
http://www.casi.org.uk/discuss/2003/msg00457.html

Simon Byers hakkında,
http://www.research.att.com/people/Byers_Simon_D/index.html
http://www.informatik.uni-trier.de/~ley/db/indices/a-tree/b/Byers:Simon.html
http://www.sans.org%2Freading_room%2Fwhitepapers%2Fprivacy%2Fhidden-data-electronic-documents_1455&ei=xnPlTdLDBYXNswbv1ICJBg&usg=AFQjCNEN7MegXSeQ5sbi1V0JNIMCgtYgeQ

Adli Bilişim yazınına giren örnek olay
H.Carvey, Windows Forensics and Incident Recovery, Addison-Wesley, 2005 sayfa,99

E.Casey, Digital Evidenceand Computer Crime, Forensic science, Computer&The Internet, Elsevier, 2004

B.Carier, File system Forensic Analysis, Addison-Wesley, 2005

k.J.Jones, R.Bejtlich, C.W.Rose, Real Digital Forensics, Computer Security and Incident Response, Addison-Wesley, 2006

S.Bunting, W.Wei, Encase Cretified Examiner Study Guide, Wiley, 2006

C.Ceylan, Bilgi Teknolojileri Kapsamında Ulusal Güvenlik ve Şirketlerin Durum, yayına hazırlanıyor.

Ofis belgelerinde gizli bilgiler,
http://news.bbc.co.uk/2/hi/uk_news/magazine/3154479.stm

Qing Wang tarafından Blackhat DC 2010 da, yapılan, Ofis Belgeleriyle Savaş: "MS Office War" sunumu
*www.pediy.com/megatron/**black_hat**_slides_final.pdf*
http://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html

USB bellekler ile ilgili EGM açıklaması ve haberler
http://www.sondakika.com/haber-emniyetten-aciklama-flash-bellekler-ayni-marka-2671872/
http://www.hurriyet.com.tr/gundem/17617840.asp
http://www.sabah.com.tr/Gundem/2011/04/23/hkim-ayni-seri-numarali-iki-flash-bellegi-istedi
http://www.zaman.com/yazdir.do?haberno=1124829

***Otomatik ıslak imza hakkında**,*
http://www.realsig.com/index.htm
http://www.nytimes.com/2011/05/28/us/politics/28sign.html?_r=2&scp=5&sq=obama&st=cse
http://www.hurriyet.com.tr/planet/17901977.asp