ULUSLARARASI BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI (ISCTURKEY 2012)
SONUÇ BİLDİRGESİ

Bilgi Güvenliği Derneği tarafından Gazi Üniversitesi, Orta Doğu Teknik Üniversitesi, Bilgi Teknolojileri ve İletişim Kurumu işbirliği ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı himayelerinde bu yıl beşincisi düzenlenen ISCTurkey 2012 etkinliği, 17-18 Mayıs 2012 tarihleri arasında Ankara'da ODTÜ Kültür ve Kongre Merkezinde yapılmıştır.

UluslararasıBilgi Güvenliği ve Kriptoloji Konferansı düzenlendiği ilk yıldan beri Türkiye'nin bu alanlardaki bilimsel ve sektörel çalışmaların paylaşıldığı,üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamunun bilgilendirildiği, eğitildiği, ulusal ve uluslararası tüm bilim insanları,araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişinin sağlandığı, ülkemizdeki bu alandaki en önemli etkinlik olup bilgi güvenliği ve kriptoloji kavramlarının, toplumun bireyleri tarafından özümsenmesine yardımcıolmak, ülkemizde bu alanda bilimsel bilgi birikiminin arttırılmasına katkılar sağlamak, kurumlar ve sektör arasındaki işbirliğini arttırmak ve en önemlisi bunu uluslararası boyutta yaparak katılımcıların kazanım ve katkılarıarttırmayı ve uluslararası işbirliğini arttırmayı hedeflemiştir.

Bilgi güvenliği ve kriptoloji alanlarında farkındalığıoluşturmak, ulusal ve uluslararası işbirliğini arttırmak ve siber tehdide yönelik riskler ve çözüm önerilerini geliştirmek amacıyla gerçekleştirilen bu etkinliğe 1000'e yakın kişi kayıt yaptırmış olup, kamu, üniversite, özel sektörden ulusal ve uluslararası düzeyde 800'ün üzerinde ilgili kişiler katılmıştır. Konferansın bildiriler kitabında yayınlanması için akademisyenler ve uygulayıcılar tarafından eşbaşkanlara iletilen bildiriler, alanında uzman en az iki hakem tarafından değerlendirilmiştir. Hakem değerlendirilmesi sonucunda uygun bulunan bildiriler sözlü veya poster sunumu için seçilerek bildiriler kitabında basılmıştır. Toplam 87 bildiri başvurusundan 47 adedi oral (sözlü) sunum ve 11 adedi ise poster sunumu için kabul edilmiştir. Sözlü sunum için seçilen bildiriler konferansta altı ayrı salonda; poster sunumları ise, katılımcıların görebileceği bir salonda poster olarak yazarlar tarafından sunulmuştur. Kabul edilen bildiriler ve posterler, siber güvenlik ve savunma stratejileri, steganografi, kriptografi, kriptoanaliz, protokol güvenliği, bilgi güvenliğini sağlama yöntemleri, saldırı tespit yöntemleri, IPv6 güvenliği, RFID, kablosuz ağlar, saldırı tespit sistemleri, bulut bilişim, kayıtlı elektronik posta, kuantum ve kaotik şifreleme ile akıllı kartlarda kullanılan kriptografik protokoller ve bunların uygulamalarına yönelik çalışmaları kapsamaktadır.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nın hedefleri doğrultusunda, bu sene ana teması "Siber Güvenlik ve Savunma" olarak belirlenen etkinliğin, ülkelerin askeri, ekonomik, teknolojik ve kritik altyapılarına karşı son zamanlarda büyük artış gösteren siber saldırılara karşı koyabilecek ve/veya engel olabilecek çözüm önerileri diğer konularla beraber özellikle konferans çerçevesinde konunun uzmanları tarafından değerlendirilmiştir.

Konferans açılışını Bilgi Güvenliği Derneği BaşkanıProf. Dr. Mustafa ALKAN, ODTÜ Rektörü Prof. Dr. Ahmet ACAR, Gazi Üniversitesi Rektörü Prof. Dr. Rıza AYHAN, TBMM Bilişim ve İnternet Araştırma Komisyonu Başkanı Prof. Dr. Necdet ÜNÜVAR ve Ulaştırma, Denizcilik ve Haberleşme Bakanı Sn. Binali YILDIRIM yapmıştır.

Bilgi Güvenliği Derneği Başkanı Prof. Dr. Mustafa Alkan, "uluslararası savaşların artık siber ortamda gerçekleştiğine dikkat çekerek, binlerce bilgisayarın köleleştirilip kontrol altına alındığını ve gerek ülke gerekse kişisel bilgilerin tehdit unsuru olarak karşımıza çıktığını,kişisel ve kurumsal bilgi güvenliği konusunda bilinç oluşturulması, yaşayan bir sistem olarak bilgi güvenliği olgusunun hayata geçirilmesi ve siber dünyada her türlü tedbiri almamız ve her türlü tehdit ve tehlikeye karşı hazır olmamız gerektiğini, bilgi güvenliği konusunda Bilgi Güvenliği Derneği olarak bir Koordinasyon ve Uzmanlar Kurulu oluşturduklarını, bu konuda yetişmiş insan kaynağımızı bir araya getirmek ve yine siber güvenlik konusunda bilim ve danışma kurullarını da hayata geçirerek ülkemizin siber savunmasına katkılar sağlamayı hedeflediklerini belirtmişlerdir.

Konferans süresince ana tema "Siber Güvenlik ve Savunma" konusu çerçevesinde sözlü sunumların yanında davetli konuşmalara ve çalıştaylara da yer verilmiştir.

- Dr. Rodica Tirtea (European Network and Information Security Agency) tarafından "Ulusal Bilgi Güvenliği ve Gizliliği" ve Prof. Dr. Nasir Memon (Polytechnic Institute of New York University ve Center for Interdisciplinary Studies in Security and Privacy) tarafından "Biyometrik Yöntemler ile Bilgi Güvenliği"ve Data Devastation şirketinden Joshua MARPET, Sayısal Adli Bilişim Sistemleriyle Oynama (Gaming the Digital Forensic System) başlıklarında konuşmalar yapmışlardır.
- Oturum başkanlıklarını Prof. Dr. Şeref SAĞIROĞLU'nun ve BGD YK Üyesi Ali YAZICI'nın yaptığı "Siber Güvenlik" ve"Siber Savunma" panelleri düzenlenmiştir.
- Oturum başkanlıklarını Prof. Dr. Ali YAZICI'nın yaptığı "Ağ Güvenliği",Yrd. Doç. Dr. Murat KOYUNCU'nun yaptığı "Siber Güvenlik", Yrd. Doç. Dr. Serdar PEHLİVANOĞLU'nun yaptığı "Bilgi Güvenliği", Doç. Dr. Ali AYDIN Selçuk'un

yaptığı “Kablosuz Ağlarda Güvenlik”, Yrd. Doç. Dr. Zülfükar SAYGI’nın yaptığı“Kriptografik Protokoller”, Doç. Dr. Melek Diker YÜCEL’in yaptığı“Kriptografinin Temelleri”, Prof. Dr. Ali DOĞANAKSOY’un yaptığı“Kriptoanaliz-I”, Prof. Dr. Ferruh ÖZBUDAK’ın yaptığı “Kriptoanaliz-II”, Dr. Tolga YALÇIN’ın yaptığı “Kriptografik Donanımlar ve Kuantum Kriptografi”, Prof. Dr. Ziya AKTAŞ’ın yaptığı “Kullanışlı Güvenlik ve Steganografi”, Dr. Orhun KARA’nın yaptığı “Bilgi Güvenliği” konulu bilimsel oturumlar gerçekleştirilmiştir.

- Eşbaşkanlıklarını Prof. Dr. Ersan AKYILDIZ ve Prof. Dr. Şeref SAĞIROĞLU’nun yaptığı “Siber Güvenlik ve Savunma Koordinasyon Kurulu", başkanlığınıProf. Dr. Mustafa ALKAN’ın yaptığı “Bilgi Güvenliği STK Toplantısı”,başkanlığını Alper ÖZBİLEN’in yaptığı “Güvenlik Uzmanları Kurulu" toplantıları ile başkanlığını Ezgi CANKURTARAN'ın yaptığı BGD Genç Üniversite Temsilcileri toplantısı yapılmıştır.
- Başkanlığını Doç. Dr. Sıddıka Berna Örs YALÇIN’ın yaptığı “Yan Kanal Analizi ve Gömülü Sistemler”, başkanlığını Prof. Dr. Fatoş Tünay YARMAN VURAL’ın yaptığı “Adli Bilişim ve Sayısal Sahtecilik” ile başkanlığını BGD YK üyesi Yıldız BARLAS’ın yaptığı“Elektronik Noterlik Uygulamaları ve Siber Güvenlik” konularında çalıştaylar düzenlenmiştir.
- “Ulusal Bilgi Güvenliğinde Log Yönetiminin Önemi”, “KEP Özelinde Kritik Altyapı Güvenliği ve Entegre Yönetim Sistemleri”, “VOIP Güvenliği”, “Sanallaştırma Veri Güvenliği”, “SIP Güvenliği”,“Siber Güvenlik Tehditlerine Karşı Farkındalık Geliştirme Eğitimi”, “Ağlarda Yeni Güvenlik Tehditleri”, “Cep Telefonlarında Veri Güvenliği” gibi konularda uygulamalı eğitimler verilmiştir.

Konferansımıza katılan İran Kriptoloji Derneği üyeleri ve IrakIEEE Bölümü Başkanı ile görüşmeler yapılmış ve uluslararası düzeyde ortak bilimsel faaliyetler düzenleme konusunda ön işbirliği anlaşmasıimzalanmış ve gelecek yıllarda uluslararası bilimsel işbirliğinin arttırılmasıiçin ilk adım atılmıştır.

ISCTURKEY 2012 SONUÇ BİLDİRGESİ

1. Günümüzde, firma kurumların %61 oranında kendilerini siber saldırganların hedefinde gördüğü bir ortamda, siber saldırıların %61'inin Anonymous gurubu tarafından yapıldığı, %51 oranında siber saldırganlar tarafından sürdürüldüğü, %28 oranında Çinli saldıranlar tarafından

gerçekleştiği, %13'ünün Rusya kaynaklı olduğu, siber saldırılarda Amerika'nın önde ülkeler arasında olsa da kendisini çok iyi kamufle ettiği bir dönemde bulunduğumuzu,

2. Yapılan saldırılara baktığımızda da bunların %45'inin Kötücül Yazılımlar marifetiyle yapıldığı,yeni oltalama veya sazan avlama yaklaşımlarının %16 oranında kullanıldığı, %13 oranında dosya indirme ile gerçekleştiği, %11 oranında DDOS saldırılarından kaynaklandığı ve son olarak %4 oranında da SQL Enjeksiyon yaklaşımlarından kaynaklandığı,
3. İyi bir siber güvenlik veya savunmanın sağlanması için iyi uygulamalara ihtiyaç olduğu ve daha güvenli politikalar uygulayarak güvenliğin %58 oranında sağlanabileceği, kişisel ve kurumsal gayretlerle güvenliğin %20 oranında sağlanabileceği, daha iyi teknoloji kullanarak güvenliğin %18 oranında iyileştirilebileceği, ülkesine göre ise ülke kanun ve yönetmeliklerin de siber güvenliğinin iyileştirilmesine %7 oranında katkı sağlayabileceği raporlanmış olsa da %7 oranının ülkemiz için kabul edilebilecek bir yüzde olmadığı,
4. Son zamanlarda ülkemizde ve dünyada kötücül yazılım bulaştırma, oltalama veya sazan avlama, hizmet durdurma, veritabanlarına sızma gibi siber saldırı olaylarının arttığı,siber saldırganların farklı ülke ve coğrafyalardan özel hedef seçerek veya genel taramalarla kendilerine kurbanlar seçtiği; özellikle son dönemlerde *Anonymous* vb. siber korsanların hedefli saldırılarla bazı kurum ve kuruluşlar üzerinden ses getirecek saldırılar gerçekleştirme gayretlerinin yoğunlaştığı, başta kamu olmak üzere tüm kurum ve kuruluşların birçok hizmetlerini internet ortamında sunmaya başlamasıyla birlikte bu ortamda yaşanan olumsuzlukların; BTK, TİB, Adalet Bakanlığı, EGM, İçişleri Bakanlığı, gibi kurumlara son dönemde yapılan saldırılar neticesinde bu saldırıların sosyal ve ekonomik hayatımızıönemli ölçüde etkileyebileceği, yaşanacak muhtemel siber güvenlik olaylarının kişisel ve toplumsal pek çok ekonomik ve sosyal olumsuz hususu beraberinde getirebileceği ve sonuçta telafisi güç neticelere sebebiyet verebileceği, dolayısıyla elektronik ortamdaki oluşacak kesinti veya saldırıların kişisel, kurumsal ve ulusal anlamda kabul edilemez boyutlara varabileceğinin farkında olunması, bunun tüm kesimler tarafından biliniyor olması ve gerekli önlemlerin arttırılmasının artık zorunluluk olduğu, Sayısal ortamda hizmet veren farklı kamu ve özel kuruluşların bugüne kadar gelinen süreçte kıymetli tecrübeleri bulunduğu, karşılıklı tecrübe paylaşımına imkan sağlayacak kurullarının oluşturulmasına ihtiyaç olduğu; siber saldırganların geçmişe nispetle daha organize yapılar haline geldikleri ve bu saldırılarla başedebilmek koordinasyonun ve bilgi paylaşımına ihtiyaç olduğu,

5. Ülkemize yapılan siber saldırılarla ilgili olarak yapay gündem oluşturulduğu fakat esas üzerinde durulması gereken kritik altyapılara sızma ve keşif yapma, kritik öneme haiz veritabanlarını gizlice ele geçirme gibi saldırıları ve saldırı girişimlerine karşıyapılabileceklerin ise yeterince tartışılmadığı,
6. Sunulan bildirilerden, yapılan tartışmalardan ve yapılan çalıştaylardan anlaşıldığıüzere siber güvenlik tanımı ve kapsamının iyi anlaşılamadığı bu konuda kurumların bilgi birikimlerini arttırmaları gerektiği,
7. Ağ ve bilgi sistemlerin ve varlıklarının ülke ekonomisi, kamu refahı ve güvenliği için çok önemli olduğu, dolayısıyla da siber varlıkların güvenliğinin ülke ve toplum güvenliğiyle eşdeğer olduğu, bu hususun her zaman hatırda tutularak kapsamlı ve uzun soluklu adımlar atılması ve çözümler geliştirilmesi gerektiği,
8. Siber tehdit algısının siber ortamı yoğun olarak kullanan kurum ve kuruluşlarca kısmen var olduğu fakat kapsamlı risk değerlendirmesinin kısıtlısayıdaki kuruluşlarca yapıldığı ve bu sayının arttırılmasının zaruri olduğu,
9. Kritik altyapı güvenliği konusunda ilgili kurumların çalışma yapmalarının ve koruma seviyelerini arttırmalarının gerektiği,
10. Siber güvenliğin temel unsurlarından olan güvenlik yazılım ve donanımlarının yerli olarak geliştirilmesi, konunun ülke güvenliği için stratejik öneme sahip olması nedeniyle milli üretimine daha fazla teşvik verilmesi gerektiği
11. İyi bir siber güvenlik stratejisinin oluşturulması için mutlaka bilişim kültürünün yaygınlaşması ve siber güvenlik kültürünün son kullanıcıdan, teknik personele, yöneticilerden yasa koyuculara ve son adımda da siyasi kültür oluşturulmasından geçtiğinin farkında olunması
12. Estonya (2008), Finlandiya (2008), Slovenya(2008),İngiltere (2010), Almanya (2010), Kanada (2010), İspanya (2010), Çek Cumhuriyeti (2011), Fransa (2011), Amerika (Mayıs 2011) gibi ülkelerin siber güvenlik stratejilerini 2008-2012 yılları arasında çoğunlukla yayımladıkları, ENISA'nın bunu Mayıs (2012) yayımlayarak AB ülkelerinin siber güvenlik stratejilerini oluştururken nelere dikkat etmeleri konusunda dokümanların hazır olduğu,
13. İngiltere'nin ülke bilgi varlıklarını korumak ekonomik gelişme, yatırım ve kalite bakış açısıyla siber güvenliği sağlamak ve fırsatları değerlendirmeyi hedeflediği,
14. Amerika'nın ekonomi (uluslar arası standartlarıyükseltme), ağları koruma (güvenliği geliştirme), kanun gücü, askeri (21. Yüzyıla hazır olma), internet yönetişimi (efektif ve kapsamlı yapılar oluşturma), uluslararası olarak kapasite, yetenek, güvenlik boyutunu

geliştirme, ve internet özgürlüğü (özgürlük ve kişisel verileri koruma) gibi kavramlar açısından siber güvenliği sağlamayı hedeflediği ve bunun en öncelikli konuların başında geldiği, yapılacak herhangi bir siber saldırıyı savaş sebebi sayacağını açıklaması, siber tehlikelerin boyutunu ve konuya verdiği önemin göstergeleri olduğu,

15. Kanada (2010) stratejisi incelendiğinde ise kamu kurumlarının korunması, kamu kurumları dışındaki önemli altyapıların korunmasıve Kanada'lılara online güvenlik sağlama (kişisel verileri koruma, siber suçlar koruma) gibi üç adımlık bir çözüm yaklaşımını benimsediği
16. İspanya (2010)'nın olaylara müdahale yapılarını güçlendirme, politikaları güncelleme, pasiften ziyade aktif yapılar oluşturma, ekonomik gelişmeleri destekleyecek güvenlik yapıları kurma, uluslararası işbirliği gibi konuları temel alarak siber güvenliği sağlama hedeflerinin stratejisinde bulunduğu,
17. AB'nin kısa ve uzun dönem olmak üzere iki adımda siber güvenlik stratejisi oluşturduğu;

Kısa dönemde:

a. Geliştirme, yeniden değerlendirme, bakım, siber güvenlik stratejisi ve aksiyon planı
b. Amaç ve hedeflerin belirlenmesi ve buna uygun bir siber güvenlik tanımının yapılması
c. Taraflardan gelen düşünceleri destekleme
d. Üye ülkeler ve AB komisyonu ile işbirliği
e. Endüstri-Üniversite ve Vatandaşlarla ilgili çalışmalar
f. Yaşayan ve geliştirilen bir strateji
g. Riskler-tehditler içerdiği kadar yeni fırsatlarda beraberinde getirdiği
h. Geliştirilen stratejiler kullanılması ve kaynak israfından kaçınılması
i. AB stratejilerine destek

Uzun Dönemde ise:

a. AB'nin ortak hedeflerini destekleyecek ortaklaşa kabul edilmiş siber güvenlik tanımlarını kabul ve uygulama
b. Siber güvenlik stratejilerini AB ile uyumlu hale getirilmesi ve ülkelerin hedeflerinde herhangi bir zıtlık oluşturmaması
c. Kamu ve özel sektör birlikte çalışması
d. İyi Uygulamalar Kılavuzu oluşturma

hedeflerinin bulunduğu,

18. Gelişmiş ve gelişmekte olan bir çok ülkenin kendi siber altyapılarını da dikkate alarak'Siber Güvenlik ve Savunma' stratejilerini oluşturduğu ve Ülkemizde üniversiteler,

ilgili sivil toplum, kurum ve kuruluşlarla bir araya gelerek kendi siber güvenlik stratejisini kapsamlı olarak hazırlaması ve bunun hazırlanması sırasında kamu kurum ve kuruluşlarının yanında özel sektör ve üniversitelerinde ortaklaşa çalışarak bu strateji belgesini oluşturmalarıgerektiği,

19. Ülkemizde siber güvenlik ve savunmanın artık önemli bir problem olunduğunun farkında olunduğu, Genel Kurmay Başkanlığının, Savunma Sanayi Müsteşarlığının, TÜBİTAK'ın, BTK'nın, EGM'nin, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile Bilgi Güvenliği Derneğinin kısmen işbirlikleri yaptıkları ve gerekli önlemlerin alınması için adım attıkları önemli olsa da henüz bir koordinasyon merkezinin/biriminin oluşturulmadığı bu işin ana sorumlusunun bilinmemesinin atılacak adımları geciktirdiği, bunun için de bu adımın ivedilikle atılması ve sorumlu kurumun belirlenmesi gerektiği,
20. Konuyla ilgili kararlar ve aksiyonlar alınırken kişisel veri güvenliği ve özürlüklere duyarlı ve saygılı olunarak adımların atılması, ulusal ve uluslararası siber güvenlik bakış açısıyla olayları kapsamlı şekilde bakılarak bir ülke stratejisinin belirlenmesi gerektiği,
21. Kapsamlı bir ülke güvenlik stratejisi oluşturulurken, TBMM desteğinin alınması, yeni anayasa hazırlanırken bu hususlara dikkat edilmesi, kurum ve özel sektör arasındaki ilişkilerin tekrar gözden geçirilmesi, düzenlemelerin sağlıklı yapılabilmesi için mevcut kanun ve yönetmeliklere uygunluk sağlanması,sayısal kimlik doğrulama yaklaşımlarının geliştirilmesi, kurulların ve kurumların bu bakış açısıyla modernizasyonu, politika ve düzenlemeler ile ülke bilgi güvenliğinin arttırılması, kapasite ve yetenek artırımı ile insan kaynaklarının ve mevcut bilgi birikimi ve deneyimlerin kullanılarak çözümler geliştirilmesinin önemli olduğu,
22. Siber güvenlik tehditlerine karşı koymak, mevcut bilgi birikimini, yazılım, donanım ve insan kaynağı potansiyelini arttırmak için ve mevcut kaynaklarıverimli kullanmak için koordinasyonun zorunlu olduğu,
23. Gelişmiş ülkelerde siber güvenlik politika ve projelerinin büyük ölçüde tamamlandığı, bu konuda kurumsal altyapıların tamamlanarak ilgili kurumlarca siber güvenlik çalışmalarının yürütüldüğü, Türkiye'de de ivedilikle politika ve strateji belirleme sürecinin hızlandırılması ve beraberinde kurumsal yapılanmanın gerçekleştirilmesi gerektiği,
24. Hızlı artan ve çeşitlenen tehditlere karşı etkin mücadelenin küresel ölçekte örgütlenmiş organizasyonlar eliyle yürütülebileceği, bu yönüyle siber saldırılara karşı uluslararası bilgi paylaşımı ve işbirliklerinin de önem arz ettiği, Türkiye'nin ilgili organizasyonlarla işbirliğini daha da güçlendirmesi gerektiği, hatta bu konuda bölgesel bir siber güvenlik

organizasyonunun kurulmasına öncülük etmesinin çok yerinde olacağı ve bölgede lider ülke olma vizyonunu da güçlendireceği,

25. Ülkemizde üniversitelerin siber güvenlik konusunda lisansüstü eğitimde programlar açmalarının gerekli olduğu, ilgili bölümlerde de konuyla ilgili dersler açılmasının faydalı olacağı,
26. Ülkemizde yürütülen siber güvenlik tatbikatların, bu alanda farkındalığın oluşması ve gerekli tedbirlerin alınmasına büyük katkılar sağladığı/sağlayacağı, devlet koordinasyonunda daha geniş katılımlı Siber Güvenlik Tatbikatlarının yapılmasının ve desteklenmesinin gerekli olduğu,
27. Ulusal ve uluslararası siber saldırıların izlenmesinin, muhtemel saldırıların tespiti ve gerekli tedbirlerin hızlıca alınması noktasında fayda sağlayacağı,
28. Siber saldırılarla mücadele ve gerekli savunma unsurlarının hazırlanmasıiçin gerekli yapısal düzenlemelerin ivedilikle hayata geçirilmesi gerektiği,
29. Kamu kurumları, STK'lar, sektör ve üniversitelerin beraber çalışarak siber güvenlik konusunda ihtiyaç duyulan strateji ve politikaları geliştirmesi,
30. Kurumların ve bireylerin maruz kaldıkları siber saldırılara karşı hukuki düzenlemelerin ihtiyaca cevap verecek biçimde yeniden ele alınması gerektiği,
31. Siber bilgi güvenliğini yüksek oranda sağlamada en önemli hususun başında"bilgiyi ve teknolojiyi üreten ülke" olmak gerektiğinin her zaman hatırda bulunarak gerekli adımların atılması gerektiği,
32. Gizli ve açık siber saldırılara karşı sadece reaktif tutum izlemenin yeterli olmayacağı, kısmen oluşturulan mevcut karşı savunma gücünün geliştirilmesinin ihtiyaç olduğu,
33. Kurum ve kuruluşların kendi siber savunma talimatlarının oluşturulması ve bu talimatlarda ilgili çalışanların görev ve sorumluluklarının da tanımlanmasıgerektiği, ayrıca talimattaki hususlara uyulup uyulmadığının uzman kurullarca denetlenmesinin, kurum ve kuruluşların güvenliği için önem arz ettiği,
34. Siber güvenlik ve savunma konularında bilgi birikimlerinin ve tecrübelerin paylaşımını temin etmek amacıyla kurumlar arası işbirliğinin güçlendirilmesi gerektiği,
35. Kurumların bilgi varlıklarını savunmalarına destek olmak, gerektiğinde müdahale etmek ve toplu saldırılar karşısında gerekli savunmayı yapmak ve koordinasyonu sağlamak amacıyla 'Acil Kriz Yönetimi ve Müdahale Merkezi'kurulmasının gerekliliği,
36. Elektronik ortamlarda hizmet veren veya iş ve işlemleri yürüten tüm kamu kurum ve kuruluşlar ile özel sektör kuruluşlarının uluslararası güvenlik standartlarıyla

belgelendirilmesinin artık bir zorunluluk haline geldiği ve bu hususun kısa sürede tamamlanmasının fayda getireceği,

37. Siber güvenliğin sadece teknik bir konu olarak ele alınmaması gerektiği, meselenin sosyal ve ekonomik ve ülke güvenliği boyutlarıyla birlikte değerlendirilmesi gerektiği
38. Uzman kişilerin bilgi ve becerilerinden faydalanmak amacıyla, kamuda sözleşmeli siber güvenlik uzmanlarının istihdamıyla ilgili düzenlemelerin yapılması gerektiği,
39. Kişisel kurumsal ve ulusal bazda bütüncül tedbir ve çözümlerin ortaya konulacağı siber güvenlik ulusal eylem planına ihtiyaç duyulduğu,
40. Ulusal farkındalığın arttırılmasına katkı sağlamak amacıyla ABD'de olduğu gibi "Siber Güvenlik Farkındalık Ayı" olarak kabul edilmesi ve ülkemizde "Siber Güvenlik Farkındalık Ayı" olarak kutlanması, tüm kamu ve özel sektör kurumlarının bu ayda konuyla ilgili olarak belirli bir plan dahilinde çalışmalar yürütmesinin faydalı olacağı,
41. Bilgi Güvenliği Derneği tarafından başlatılan "Siber Güvenlik Ulusal Koordinasyon Kurulu" ve "Siber Güvenlik Uzmanlar Kurulu" çalışmalarının arttırılarak devam edilmesi ve bu kapsamda ilgili birim temsilcileri ile bir araya gelinerek kısa sürede Siber Güvenlik Strateji Dokümanlarının oluşturulmasının Kurumsal, Ulusal ve Uluslararası ölçekte siber güvenlik çalışmalarının yürütülmesinin ülke siber güvenlik ve savunma stratejilerinin kapsamlı olarak oluşturulması ve geliştirilmesine büyük katkılar sağlayacağı,
42. Ülkemizde yapılan akademik çalışmalar genel olarak değerlendirildiğinde teorik çalışmaların gittikçe azalmakta olduğu, bu konuda üniversitelerin daha kapsamlı ve teorik çalışmalarda yapmalarının yerinde olacağı,
43. Ülkemizde yaygın olan ve önemli bir açığı kapatan noterlik mesleğinin elektronik noterlik ile beraber siber tehditlere maruz kalabileceği, onun içindeşimdiden bu konuda gerekli önlemlerin alınması,
44. Adli bilişim alanında yapılan çalışmaların arttırılması ve sayısal delillerin toplanması konusunda daha hassas davranılması, kişisel hak ve özgürlüklere zarar verebilecek sahte sayısal verilerin oluşturulma ve yanıltma tekniklerinin bulunduğu, mevcut sorunları gidermek için:
    - Yasa ve yönetmeliklerimiz sahte sayısal belgelerin yargıyı yanıltmasını engellemek üzere yeniden düzenlenmeli ve kaynağı belli olmayan dijital sayısal veriler değerlendirmeye alınmamalıdır.
    - Böyle hususlarla karşılaşılmaması için yeni düzenlemelere ihtiyaç olduğu, yeni yapılan anayasa da bu hususa dikkate alınmasının faydalı olacağı,

- Hukuk Fakültelerimizde Adli Bilişim konuları ve bilişim teknolojileri müfredat programlarına alınmalı ve hukukçularımız bilirkişi raporlarını anlayacak, değerlendirecek ve yorumlayacak bir bilgi düzeyine getirilmelidir.
- Adli Bilişim uzmanlarımızın bilgi düzeylerinin arttırılması için adli bilişim sertifika programları içerikleri güncellenmelidir.
- Üniversitelerimizde Adli Bilişim Anabilim dalları kurulmalıdır.
- Türkiye'de bağımsız bir Adli Bilişim Kurumu kurulmalıdır.

45. Bilgi güvenliği kavramlarını sağlamak amacıyla kamu kurumlarında kullanılan kriptografik modül içeren cihazların test ve sertifikasyonu için varolan laboratuvarların (TSE'den onaylı) sayısının arttırılması ve burada üniversitelerin ilgili birimlerinde yüksek lisans/doktora yapmışaraştırmacıların çalışmasının teşvik edilmesi,
46. Üniversite ve kamu kurumlarındaki araştırmacıların Siber Güvenlik alanındaki akademik çalışmalarını arttırmak amacıyla, aynı Avrupa Birliği FP7'de olduğu gibi öncelikli alanlar içerisine Bilgi Güvenliği ve Kriptoloji alanının eklenmesi,
47. Kamu kurumlarının bilgi işlem birimlerinde çalışan personelin siber güvenlik alanında kısa süreli eğitimler almasının faydalı olacağı,
48. Bu konferansta elde edilen tüm çıktılar (sunumlar, bildiriler kitabı,eğitim materyalleri, videolar) toparlanarak her konferans sonunda olduğu gibi ücretsiz olarak kamuoyu ile paylaşılmakta olup konferans hakkında detaylıbilgiler ile sunulan bildiriler ve davetli konuşmacıların sunumlarına www.iscturkey.org adresinden erişilebilinir.

Kamuoyuna saygıyla duyurulur.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı 2012 Düzenleme Kurulu