**التبعات القانونية في مجابهة شبكة البرامج الخبيثة**

**المقدمة**

اهداف المهاجمين تهدف الى التركيز على الربح المادي. حيث إنه يقدر بان البوت نت [[1]](#footnote-1)(Botnet) تولد دخل ما بين 10.000 الى 10.000.000 دولار امريكي في الشهر لكل بوت نت[[2]](#footnote-2) .رؤية هذه الارقام تساعد المرء على فهم لماذا أصبحت الان البرمجيات الخبيثة صناعة اجرامية عالمية وتعطي دلالة على عدد المصادر التي يمكن استثمارها في تطوير برمجيات خبيثة جديدة ومعقدة حيث تكون مقاومة لجهود اكتشافها او احتوائها. ونتيجة لذلك، ظهرت السوق السوداء حيث تستخدم البوت نت كخدمات يمكن شرائها و تعديلها وتأجيرها.

بالاضافة الى ذلك، فقدت ازدادت هجمات البوت نت ذات الدافع السياسي وأصبحت محط الاهتمام الدولي. في 2007، تم استخدام البوت نت لاطلاق هجماي الدي دوس ضد المواقع الاستونية الحكومية و مواقع القطاع الخاص. و في خلال الصراع الروسي الجورجي في عام 2008 ، تم استخدام البوت نت للحد من قدرات جورجيا على نشر المعلومات عن الصراع العسكري الجاري على عامة الشعب الجورجي و العالم الخارجي.. كما ان البوت نت من الادوات السهل الوصول اليها من قبل المهكرين لأغراض سياسية حيث يستخدمونها لدعم اراءهم ذات الطابع السياسي، مثل ما حصل في مهاجمة مفاعل نتانز الايراني والنجاح فى ايقاف عمل المفاعل وإلحاق الاضرار فى اجهزة الطرد المركزي باستخدام برمجيات خبيثة Stuxnet.

انه من الصعب قياس مقدار العدوى العالمية التي تصيب الحواسيب من قبل البرمجيات الخبيثة. على سبيل المثال فان شركة ميكروسوفت قامت بقياس متوسط مقدار العدوى العالمية من 7.1 على مقياس 1000 جهاز حاسوب كنتيجة لتنظيفهم بأداة ميكروسوفت المجانية المزيلة للبرمجيات الخبيثة في الربع الثاني من عام [[3]](#footnote-3)2011. ومن المحتمل ان هذا الرقم قليل جدا حيث ان ليس كل مالك لنظام ويندوز يقوم باستخدام هذا البرنامج كمان ان معدل اكتشاف البرمجيات الخبيثة ليس مرتفع عموما. و على الرغم من ذلك فان الارقام لا زالت تعطي انطباعا اوليا. مؤسسة (ShadowServer Foundation) عبارة عن مجموعة من المتطوعين ذووا خبرة عالية في مجال الامن و ومحاربة البرمجيات الخبيثة وبالاخص البوت نت. حيث اكتشفوا حوالي 5500 بوتنت مختلف في فبراير 2012[[4]](#footnote-4). وهذا يوضح بشكل كبير حقيقة الخطر المحتمل من هجمات البوت نت بشكل هائل.

للتلخيص، فقد تحول البوت نت الى اداة قوية لكل من المجرمين والجهات الفاعلة سياسيا.[[5]](#footnote-5) و في نفس الوقت، فان انشاء وتشغيل البوت نت سهل جدا بالنظر الى توفر التعليمات والادوات في السوق السوداء. فان قلة الوعى او جهل مستخدمي الحواسيب بما يتعلق بامن الحاسوب يدعم الانتشار الواسع لبرمجيات خبيثة جديدة علي الرغم من كون انظمة الحواسيب مؤمنة جيدا ومحدثة فانها لا تكون قادرة على مقاومة احدث البرمجيات الخبيثة. كما ان شركات المضادة للفيروسات (البرمجيات الخبيثة) تجد صعوبة في التعامل مع الاعداد الكبيرة الجديدة من البرمجيات الخبيثة كل يوم.

غير انه في السنوات الاخيرة الماضية، كان هناك انتشار سريع للإنترنت وزيادة هائلة في الخدمات المرتبطة به. و نتيجة لذلك اصبح هناك زيادة في الجرائم الالكترونية المنظمة. وبذلك تحولت البوت نت Botnet الي صناعة متعددة الاوجه و سرية ولها سوقها السوداء و تعود بالربح الوفير على المجرمين الالكترونيين. يتم استخدامها للقيام بأنشطة غير قانونية مثل سرقة المعلومات الشخصية والمالية بشكل واسع، وهجمات البريد المزعج Spam ، و هجوم رفض الخدمة DDos لجعل الخدمات غير متاحة للمستخدمين. كما ان Botnet تم استخدامه في معظم الهجمات الالكترونية على نطاق واسع و التي شهدها العالم حتى يومنا هذا. مثل هجمات رفض الخدمة ضد استونيا في عام 2007 وضد جورجيا في عام 2008[[6]](#footnote-6). بالإضافة الى استخدام Botnets من قبل المعارضين الالكترونيين لإيصال رسائل معينة.

وبشكل يومي يستخدم متخصصي امن المعلومات تقنيات متعددة لاكتشاف ومعالجة البرمجيات الخبيثة على الرغم من ذلك يبدو انه يوجد شك كبير بشأن المتطلبات والقيود التي ينص عليها القانون والتي يجب الأخذ بها بعين الاعتبار عند استخدام كل تقنية من قبل المتخصصين. ولذلك يناقش هذا البحث طرق محاربة Botnet من وجهة نظر قانونية من اجل تغطية المشاكل القانونية المحتملة المتعلقة بكل تقنية.

يقوم البحث بإعطاء نظرة شاملة عن تطور التشريع القضائي الجنائي للاتحاد الاوروبي المتعلق بمحاربة البرمجيات الخبيثة Botnet. ومن ثم يناقش التقنيات و الطرق الي تكافح Botnet من خلال اعطاء تحليل لهم في ضوء التشريع في بلدين عضوين من بلدان الاتحاد الاوروبي وهما استونيا و المانيا. حيث إن ألمانيا تمثل الأمة المؤسسة للاتحاد الاوروبي و المعروفة بحمايتها القوية للحقوق الاساسية و بالأخص (الخصوصية) و من جهة أخرى فإن استونيا والتي هي عضو حديث بالاتحاد الاوروبي معروفة من حيث ابداعها في مجال انظمة تكنولوجيا المعلومات و انظمة البنية التحتية ومرونتها. ولذلك تم اختيار هاتين الدولتين للبحث.

على الرغم من ان التحليل يعتمد بشكل اساسي على قوانين كل من المانيا واستونيا ، يجب الاخذ بعين الاعتبار بان التشريعات لمجتمع المعلومات لكل من استونيا والمانيا يعتمد بشكل كبير على تشريعات الاتحاد الاوروبي و ان نصوص العقوبات القضائية للمخالفات الالكترونية تم تطويرها مع الاخذ بعين الاعتبار المتطلبات المنصوص عليها في اتفاقية الاتحاد الاوروبي بما يخص الجرائم الالكترونية – اتفاقية بودابيست[[7]](#footnote-7). ولذلك فان العديد من المشاكل والحلول التي سيتم التطرق اليها من الممكن ان تكون عامة نوعا ما خاصة بما يتعلق بالاتحاد الاوروبي.

**الخلفية التنظيمية لسياسة الاتحاد الاوروبي**

**التوجه نحو تجريم الانشطة ذات الصلة بالبرمجيات الخبيثة Botnet**

مبادرات الاتحاد الاوروبي ذات العلاقة بمكافحة البوت نت botnet تقع بشكل اكبر في اطار اجراءات الاتحاد الاوروبي بما يتعلق بمجتمع المعلومات ككل. حيث يشكلون الاطار النظري القانوني للاتحاد الاوروبي[[8]](#footnote-8) و النصوص القانونية حيث انه لا يوجد الزام بها من قبل الدول الاعضاء في الاتحاد الاوروبي. يحتوي هذا الجزء من البحث على نظرة عامة مختصرة عن هذه المبادرات التي تتعامل بشكل مباشر و عموما بغير مباشر مع محاربة البرمجيات الخبيثة Botnet وكيف ان هذه المبادرات شكلت الخلفية القانونية للاتحاد الاوروبي بما يتعلق البوت نتBotnet حتى هذا اليوم و ماهي النتائج المتوقعة من التطور الحالي في الاتحاد الاوروبي.

في مناقشات اجتماع الهيئة[[9]](#footnote-9) للاتحاد الاوروبي عام 2001 بعنوان "*الاتصالات وامن المعلومات :مقترح لنهج السياسة الاوروبية*"، صنف الاتحاد الاوروبي ثلاث مجالات لسياسة مختلفة ولكنها مترابطة من ناحية مجابهة التحديات التي يواجها مجتمع المعلومات : سياسة الاتصالات الموجودة حاليا و الاطر النظرية لحماية البيانات، السياسة المتعلقة بالجرائم الالكترونية، والسياسة التي يتم تطويرها والمتعلقة بمعايير شبكة الحاسوب وامن المعلومات(NIS) ، والتي تعالج المخاوف المتزايدة من التجسس الالكتروني (بدافع اقتصادي او سياسي او علمي) و الهجمات الالكترونية المحتملة على البنية التحتية و التي تهدد الامن القومي.

وتعريف شبكة الحاسوب وامن المعلومات(NIS)[[10]](#footnote-10) "*قدرة شبكة الحاسوب او نظام المعلومات على المقاومة الى حد موثوق به ضد الحوادث العرضية أو الاجراءات الخبيثة التي تهدد وجود و صحة وسلامة وسرية البيانات المخزنة او المنقولة والخدمات ذات الصلة المقدمة من قبل او يمكن الوصول اليها من خلال هذه الشبكات والانظمة*". ولادة سياسة أوروبية داعمة لمشروع شبكة الحاسوب وامن المعلومات NIS،أظهر تطور الحاجة لوجود اهمية تفعيل الامن الالكتروني ليخدم الامن القومي ووجب مواكبة هذا التطور على هذا الاساس. في الاعوام ما بين 2004-2006 ، تم التنسيق لتطوير نهج لسياسة للاتحاد الاوروبي لحماية أنظمة البنية التحتية الحساسة (CIIP) (مثل، انظمة التي تتحكم بالجسور والقطارات وشبكات المياه والصرف الصحي ومحطات الطاقة والانظمة العسكرية ) و قد تم تبني التشريع الاول بخصوص حماية انظمة المعلومات للبنية التحتية الحساسةCIIP في عام 2009.

حيث ان الاتصالات الالكترونية ، و حماية البيانات ، و الجريمة الالكترونية و حماية انظمة المعلومات للبنية التحتية تعتبر مجالات مستقلة في ما يتعلق بالنصوص القانونية المتعلقة بها. و في المقابل فان مشروع NISبدلا من معاملتها كفئة منفصلة ، يجب رؤيتها على انها اطار نظري لسياسة شاملة تسعى لتحقيق منظومة شاملة لتحديات الامن الجديدة. ولذلك يمكن القول بان التشريع الاوروبي في تعامله مع مجتمع المعلومات يقسم الى ثلاث فئات[[11]](#footnote-11)، وكل هذه الفئات تقع على الاقل تحت مظلة سياسة مشروع NIS.

1. الاطار التنظيمي للاتصالات الالكترونية و حماية البينات

2. الوثائق التي تتعامل مع الجرائم الالكترونية

3. معايير حماية انظمة المعلومات للبنية التحتية

من منظور مكافحة شبكات Botnet، فان الفئات الثلاثة مهمة حيث انهم يعتبرون لضمان تجريم الانشطة الخبيثة التي يتم شنها من خلال Botnet، في توافر سجلات عن الهجوم مستخلصة من الاجهزة المتضررة والمصابة لاستخدامها في التحقيقات، وهذه السجلات تحتوي على بيانات شخصية يتوجب حماية البيانات الشخصية خلال التحقيق[[12]](#footnote-12) ، مشاركة المعلومات الموجودة واليات التعاون بين دول الاعضاء ومؤسسات تنفيذ القانون.

وان التهديدات التي فرضتها Botnet خصيصا فرضت تشريع هام في السنوات الاخيرة. ولكن قد تم ذكر Botnet في سياق نشر البرمجيات الخبيثة في 2006 [[13]](#footnote-13). في خلال ذلك الاطار الزمني ،بدأ الاستعمال الاجرامي لـ Botnet بالحصول على اهتمام خاص. ولكن قبل العام 2006، فان وثائق الاتحاد الاوروبي اشارت اكثر من مرة الى الاثار التخريبية باستخدامBotnet لبدء هجوم رفض الخدمة (DDos) مما دفع الاتحاد الاوروبي الى اتخاذ اجراءات بهذا الخصوص.

**الجريمة الالكترونية**

تم ادراج قضية الجريمة الالكترونية كقضية مهمة على اجندة الاتحاد الاوروبي في عام 1999 ، حينما عقدت قمة المجلس الاوروبي ال 36 في تامبرى[[14]](#footnote-14). واختتمت القمة بأنه يجب بذل الجهود للاتفاق على تعريفات مشتركة وعلى اسس للتجريم والعقوبات في القطاعات ذات الصلة (امن المعلومات) مثل قطاع الجريمة الالكترونية[[15]](#footnote-15). تم اتباع الارشادات عام 2000 في المجلس الاوروبي والمفوضية الاوروبية [[16]](#footnote-16) وعنوان الجلسة اوروبا الرقمية 2000. حيث ان خطة العمل التي دعت الى تنسيق افضل لمحاربة الجريمة الالكترونية – نوع جديد من الجريمة عن طريق استخدام الادوات من قبل مطورين السوق السوداء. الخسائر الاقتصادية التي سببها تعطيل وظائف الانترنت على سبيل المثال ان هجمات رفض الخدمة DDOS اخذة بالارتفاع[[17]](#footnote-17). وبما انه يوجد هناك بدائل Botnet لشن هجمات DDOS ، فان الهجمات التي حازت على انتباه صائغي القرار لم تكن بالضرورة الهجمات التي تم شنها بواسطة Botnet. وبسبب ذلك ففي النهاية فان اي تشويش على النظام المعلوماتية تم تجريمه وهذا يعني بان التجريم يتم بغض النظر عن الادوات المستخدمة. وارتأت خطة العمل بان منهجية اوروبية منسقة ومتسقة لمحاربة الجريمة الالكترونية سيتم انشاءها في نهاية العام 2002.

في بداية العام 2001، اصدرت الهيئة الاوربية مذكرة لإنشاء مجتمع معلوماتي اكثر امانا من خلال تحسين بنية امن المعلومات ومحاربة الجريمة المتعلقة بأجهزة الحواسيب[[18]](#footnote-18). في المذكرة، وعدت الهيئة بان تطرح مقترح تشريعي حول تقريب القوانين المحلية حول الجرائم الالكترونية، و التأكيد على تجريم القرصنة الالكترونية وهجمات DDos مهم جدا (بسبب الخسائر الاقتصادية). كذلك سيقدم المقترح تعريفات موحدة للاتحاد الاوروبي في هذا المجال. اقتراح الهيئة في يونيو 2001 بخصوص وضع منهجية لسياسة الاتحاد الاوروبي لشبكة الحاسوب امن المعلومات ، أكدت على ان التشريع الذي سبق ذكره سيتم تطويره.[[19]](#footnote-19) ونتيجة لذلك، في ابريل 2002 ، قدمت الهيئة عرضا للمقترح للمجلس لأخذ قرار وصياغة الاطار النظري له بخصوص[[20]](#footnote-20) الهجمات ضد انظمة المعلومات. وفي تلك الاثناء، فان الهجمات الارهابية للحادي عشر من سبتمبر اجبرت الاتحاد الاوروبي على مراجعة طرقه الاستراتيجية بخصوص الارهاب الدولي. وهذا أثر على التخطيط لأخذ قرار على الاطار النظري حيث اصبح من الاولوية بان يكون التشريع الجنائي للدول الاعضاء مهيأ لمعالجة الارهاب الالكتروني.

التأكد من تناسق القانون الجنائي من خلال قرار الاطار النظري جاء لضمان ان التشريعات المحلية متجانسة الى حد حاسم وبذلك فإنها مهيأة بشكل متساوي لتأييد ملاحقة الجرائم الالكترونية العابرة للحدود من خلال تمكين التعاون بين منفذي القانون في الدول الاعضاء و السلطات القضائية. كما ان تقريب القوانين الجنائية يساعد على تجنب انتقاء مكان الهجمات حيث ان المجرمين عادة يختارون ان يقوموا بالهجمات من احد بلاد الاعضاء التي لا تدين افعالهم قانونيا او تكون العقوبات اقل من البلدان الاخرى. ولذلك فان المقترح لأخذ قرار الاطار النظري فيه ارتاء تجريم اثنين من الافعال المؤذية: الوصول غير القانوني لأنظمة المعلومات و التشويش غير القانوني علي أنظمة المعلومات. لقد استغرق المجتمع الاوروبي ثلاث سنوات ليتبنى اخيرا الاطار النظري لهذا القرار.[[21]](#footnote-21) وبما يخص الجريمة الثانية فقد تم تقسيم القرار الخاص بها الى ثلاث بنود ،وبذلك تم تقديم ثلاث احكام ، والتي من المفترض ان يتضمنوها جميع الدول الاعضاء لقوانينهم المحلية:

**البند 2** : الوصول غير القانوني لأنظمة المعلومات

**البند 3** : التشويش غير القانوني على الانظمة

**البند4**: التشويش غير القانوني على البيانات

"الوصول غير القانوني" تعني ، الوصول من غير حق لكل او اي جزء لأنظمة المعلومات، وبالتالي حماية سرية انظمة المعلومات .اما "لتشويش على الانظمة" يشمل المنع والاعاقة المتعمدة لوظائف نظام المعلومات [[22]](#footnote-22)، واما "تشويش البيانات" يشمل على الضرر المتعمدة بالبيانات من خلال و اتلاف او تغيير او حذف او تمكين الوصول الى بيانات الكمبيوتر لا يمكن الوصول اليها من خلال نظم المعلومات. التشويش غير القانوني على الانظمة المعلوماتية بالأخص هو عبارة عن فقرة تتناول هجمات رفض الخدمة . ومن جهة اخرى فان القرصنة ، تقع تحت بند الوصول الى انظمة المعلومات او التشويش غير القانوني على البيانات ، بالاعتماد على طبيعة الاجراء الذي تم اخذه.

لضمان منهجية متناسقة في التطبيق ، فان قرار الاطار النظري نص علي تعريفات للمصطلحات "نظم المعلومات" و "بيانات الحاسوب". كما انه ايضا الزم الدول الاعضاء بإقرار عقوبة على استخدام التشويش الغير القانوني على الانظمة و البيانات بعقوبات جنائية بحد اقصى وعلى الاقل السجن لمدة تتراوح ما بين عام الى 3 اعوام. كمان ان الدول الاعضاء مطالبة بأخذ المعايير الضرورية للامتثال الى تطبيق قرارات الاطار النظري بحلول مارس 2007.

في أواخر العام 2006، أشارت المفوضية الى Botnet في " *مذكرة البريد الالكتروني غير المرغوب به او المزعج Spam*"[[23]](#footnote-23) كوسيلة لإرسال رسائل البريد الالكتروني غير المرغوب بها (ترسل عشوائيا ويكون محتواها غالبا برمجيات خبيثة او عروض مزيفة) ، وبالإشارة الى ان Botnet يعتمد 50% تقريبا على رسائل بريد الكتروني الضارة التي تصيب المستخدمين من حول العالم . في مايو 2007، أصدرت المفوضية مستندا أخر حول الجريمة الالكترونية، و كان هذا المستند يهدف الى انشاء السياسة العامة لتحسين مستوى التنسيق الدولي و الاوروبي في محاربة الجريمة الالكترونية.[[24]](#footnote-24) في المستند، تم الاشارة الى Botnet على انها الوسيلة الاكثر انتشارا للقيام بهجمات ذات نطاق واسع ضد انظمة المعلومات ، الافراد، المؤسسات ، الدول. و أشار الى ان الهجمات الالكترونية يمكن توجيهها أيضا ضد انظمة البنية التحتية الحساسة للأوروبيين ، وعلى الاغلب فذلك سيؤدي الى نتائج كارثية على المجتمع ككل. لا يخفى على احد بان هذه التصريح ليس بجديد ،و لكن هذه المرة كان التأثير نابع من حادث الكتروني حقيقي و ليس من تهديد افتراضي ، و هو هجمات رفض الخدمة واسعة النطاق التي استهدفت استونيا في ابريل-مايو 2007 (الذي شل وعطل كافة انظمة الاعلامية والبث والانظمة المالية و المصرفية لمدة 3 اسابيع – مما نتج عنه حالة من الهلع بين المواطنين والفوضى عمت ارجاء البلاد). كما اكدت المذكرة على ان توحيد التشريع الجنائي للدول الاعضاء سيبقى هدف طويل المدى للاتحاد الاوروبي[[25]](#footnote-25).

تم اتباع قرار الاطار النظري بتقرير تقييمي من المفوضية الى المجلس حول ما تم تطبيقه في يوليو 2008. [[26]](#footnote-26) وأشار التقرير الى ان الدول الاعضاء قد طبقت التشريع الجنائي بطرق مختلفة. كما انه وضح بان على الرغم من الاختلافات ، فان مستوى طرق التطبيق كانت جيدة بشكل عام. وأهم من ذلك ، ويرجع ذلك الى حقيقة ان المجتمع الأوروبي قد اصيب بصدمة بسبب الهجمات التي وقعت ضد استونيا (مما دفع اعضاء الناتو –قسم الدفاع الالكتروني بإنشاء قاعدة في استونيا ونقل الكوادر المتخصصة للتعامل مع الازمة آن ذاك) ، فان التقرير التقييمي قد مهد الطريق لتشريع اوروبي جديد والذي تم تحضيره ليقوم بمعالجة التهديدات بشكل فعال وخاصة التهديدات الناجمة عن استغلال Botnet. ولمح التقرير بانه قد تم الاخذ بعين الاعتبار تجريم الانشطة التي تسهل الاستخدام الاجرامي لـ Botnet و تشديد العقوبات على انشطة التشويش على الانظمة.

وقبل ان يصدر الاتحاد الأوروبي مقترحه عن التشريع الجديد المتعلق بالجريمة الالكترونية ، فقد تم ذكر Botnet في مبادرة CIIP كما ان مذكرة المفوضية حول CIIP ذكرت ان Botnet هو تهديد للأمم، وانظمة البنية التحتية للمعلومات الحساسة، كما تم التوضيح في المثال عن استونيا، ولذلك يجب التعامل معه وفقا لذلك.

**اللوائح القانونية ضد Botnet**

في نهاية سبتمبر 2010، اصدرت المفوضية مقترح حول انشاء لوائح قانونية تعاقب كل من يقوم او يتورط بالهجوم ضد الانظمة المعلومات[[27]](#footnote-27) . والتي يشار اليها باللغة العامية "*الارشادات القانونية للبوت نت*". والتي حين تبنيها ستقوم بإبطال قرار الاطار النظري حول الهجمات ضد انظمة المعلومات. الهدف العام للتعليمات هو *" منع حصول ، وتقليل عدد الهجمات ذات النطاق الواسع والتي تصدر من او تستهدف الاتحاد الأوروبي*"[[28]](#footnote-28). من خلال ملاحقة و ادانة المجرمين وتحسين التعاون عبر الحدود وبين هيئات تطبيق القانون. على الرغم من ذلك، فان الاحكام المقترحة من قبل المفوضية عرضة للتغير في مرحلة التشريع. على سبيل المثال، اللجنة الاوروبية الاقتصادية و الاجتماعية [[29]](#footnote-29)، في رأيها حول مقترح المفوضية تدعو الى عقوبات اكثر صرامة، وبذلك فان صرامتهم تعكس خطورة الجريمة و تشكل رادع للمجرمين.[[30]](#footnote-30) وبشكل عام ، فقد أكدت اللجنة على أهمية تبني منهجية شاملة ومستقبلية لا تتعامل فقط مع تطبيق القانون والعقاب ولكن المنع من خلال معايير امنية افضل ، ومن خلال التحري والتعليم، من خلال زيادة الاستثمار في الابحاث والتطوير. اقترحت اللجنة ان تجعل امن الانترنت تحت السيطرة المركزية. حيث ان السلطة المركزية ستقوم بإنشاء معايير لأدوات انتقالية سهلة للغاية و انظمة الحاسوب ،و المواقع الالكترونية و امن البيانات.

حيث ان المقترح حول اللوائح القانونية ضد botnet يشرح مواطن الضعف في الاحكام التي قدمت في قرار الاطار النظري، و التي هي اولا: انهم لا يعالجوا الخطر المحتمل لـBotnet، وثانيا، انهم لا يأخذوا في عين الاعتبار و بشكل كاف حجم خطورة الجرائم الالكترونية وعقوباتها. ولمعالجة النواقص المحددة ، يقدم المقترح جنحتين جديدتين أساسيتين. الاعتراض غير القانوني، حيث يتم تجريم الاعتراض لنقل بيانات الحواسيب غير العامة. والجنحة الثانية، تهدف الى معاقبة انتاج و ببيع او توريد بهدف الاستخدام او تصدير او تشويش او جعل اي برنامج الكتروني للحاسوب متاحا (السوق السوداء) ، كما انه يغطي مفهوم Botnet، و ارتكاب الجرائم في التعليمات. كمان انه سيجرم ايضا التجارة الضارة بكلمات المرور و والبرامج الخبيثة والبرامج التي تنتهك خصوصية المستخدم.

وفيما يتعلق بالعقوبات، فان الحد الاقصى لعقوبة السجن سيكون عامين على أقل تقدير. ولكن اذا تم التشويش على الانظمة او البيانات ضد عدد كبير من انظمة الحواسيب ، مثل هجمات Botnet ، فان الحد الاقصى لعقوبة السجن سيكون لمدة ثلاث سنوات على الاقل. العقوبة الاكثر شدة بالسجن على الاقل مدة خمس سنوات ستكون متوقعة عند حصول الحوادث التالية: التشويش على النظام او البيانات، والذي يتم ارتكابه من خلال جهة تنظيم اجرامي متسببة بأضرار بليغة ضد البنية التحتية لأنظمة للمعلومات .

علاوة على ذلك، فان الارشادات القانونية للبوت نت تهدف الى تحسين التعاون الاوروبي حول القضايا الجنائية من خلال تقوية النظام الحالي 24/7 جهة اتصال.[[31]](#footnote-31) وتضمن على الزام بتزويد تغذية راجعة خلال ثمان ساعات للطلبات العاجلة. من المحتمل ان تكون التغذية الراجعة سلبية ايضا ، عن طريق رفض تقديم المساعدة للشخص الذي قام بالطلب- ولكن الشيء المهم هو استلام التغذية الراجعة بشكل سريع نسبيا. كما تتطلب التعليمات ايضا من الدول الاعضاء القيام بجمع بيانات احصائية حول الجريمة الالكترونية مثل عدد المخالفات التي تم تسجيلها وعدد الأشخاص الذين تم ملاحقتهم قضائيا وتم ادانتهم على المخالفات المنصوص عليها في الارشادات القانونية للبوت نت.

سيتم الزام الدول الاعضاء بنقل احكام التعليمات الى قوانينهم المحلية خلال مدة لا نزيد عن عامين من تبني الاحكام. وبأخذ ذلك بعين الاعتبار، ان تبني التعليمات من قبل الاتحاد الاوروبي سيستغرق وقتا. ومنذ تلك اللحظة سيكون لدى الدول الأعضاء عامين الي حين ادخالهم الى الاحكام المعمول بها ، كما ان تأثير الارشادات القانونية للبوت نت يمكن قياسه فقط بعد بضع سنوات. ستكون الارشادات القانونية للبوت نت قد حققت اهدافها و حتى أكثر من ذلك اذا قامت اولا بتحقيق الاهداف المباشرة لمواجهة التهديدات التي يشكلها البوت نت ولكن ثانيا بان تكون احكامها نظرية بشكل كاف حتى يكون من السهل تطبيقها على اشكال جديدة من الجريمة الالكترونية والتي لا زالت غير معروفة لنا ولكن ستظهر بالمستقبل.

**التشريع الاوروبي واتفاقية المجلس الأوروبي حول الجريمة الالكترونية**

ومن القضايا ذات الصلة، الانشطة التي يقوم بها الاتحاد الأوروبي لمكافحة الجريمة الالكترونية وكيفية توافقها مع اتفاقية المجلس الأوروبي حول الجريمة الالكترونية.[[32]](#footnote-32) والتي تعرف ايضا باتفاقية بودابست ، والتي تم عرضها للتوقيع في عام 2001 ودخلت حيز التنفيذ في عام 2004. وحتى اليوم، تم التوقيع على الاتفاقية من قبل 47 دولة من ضمنها الدول السبع وعشرين الاعضاء في الاتحاد الأوروبي ، وتم التصديق عليها من قبل 32 دولة. من الخمسة عشر التي لم يصدقوا على الاتفاقية 9 دول اعضاء في الاتحاد الأوروبي. وتحمل اتفاقية بودابست ثلاث اهداف وهي : توحيد القانون المحلي الجنائي بشكل موضوعي ، تزويد قانون الإجراءات الجنائية المحلية بالصلاحيات اللازمة للتحقيق وملاحقة الجرائم الإلكترونية و انشاء سلطة تعاون دولية سريعة وفعالة.[[33]](#footnote-33)

لقد أخذ الاتحاد الأوروبي بعين الاعتبار الاتفاقية في كل مبادرة تم اطلاقها، ولكن المواقف التي اتخذها الاتحاد الأوروبي تختلف في التركيز على ضرورة الاتفاقية و تشجيع الدول بالانضمام اليها توضيح خيبة أمل الاتحاد بسي الاعداد القليلة التي قامت بالتصديق خلال المدة الطويلة التي دخلت فيها الاتفاقية حيز التنفيذ. و الاعتراف بالحاجة الى ادوات بديلة .خطة العمل eEurope 2002 ،والتي تم تبنيها في العام 2000، قامت بالإشارة سابقا الى ان المجلس الاوروبي في خضم مناقشة اتفاقية عن الجريمة الالكترونية و أكدت على اهمية التأكد من حصول هذه المناقشات ومن حصول التعاون حول هذه القضية. [[34]](#footnote-34) وفي نفس العام ، ارتأى الاتحاد الحاجة الى تقريب القانون الجنائي على مستوى الاتحاد الأوروبي. ولكن كانت النية منذ البداية بذل الجهود حول اتفاقية الجريمة للإلكترونية. [[35]](#footnote-35) وفي المذكرات حول وضع السياسة العامة حول مكافحة الجريمة الالكترونية ، شجعت الهيئة الدول الاعضاء التي لم تقدم على التصديق على الاتفاقية بعد- " الوثيقة الأوروبية والدولية السائدة في هذا المجال"- لفعل ذلك[[36]](#footnote-36) كما ان قرار الاطار النظري ذكر ان قرار الاطار النظري سيكون متسق مع المنهجية المتبعة في اتفاقية الجريمة الالكترونية.[[37]](#footnote-37)

وضع برنامج ستوكهولم بعض الضغط على الدول الاعضاء ، داعيهم الي المصادقة على ***اتفاقية بودابست*** في اقرب وقت ممكن.[[38]](#footnote-38) هذا التشجيع تم تكراره في المقترح لـ" الارشادات القانونية للبوت نت" حيث ان الهيئة و بشكل متواضع شاركت واعربت عن خيبتها في اعداد دول الاعضاء القليلة التي قامت بالتصديق على الاتفاقية. وعلى الرغم من ان الهيئة كانت تسعى لإضافة تشريع جديد في مقترحها و التي حين يتم تبنيه سوف يفقد الحاجة الى الدول الاعضاء للمصادقة علي الاتفاقية. كانت الهيئة لا تزال تدفع بالدول الاعضاء الى فعل ذلك. وعلى الارجح كان ذلك محاولة لمنع وضع الوثيقتين في تباين وعلى الاغلب بالأخذ في عين الاعتبار حقيقة ان التشريع الأوروبي سيستغرق سنوات عدة قبل ان يتم تبنيه. واشار تقييم الاثر المرافق للمقترح بان على اجراء الاتحاد الأوروبي الاخذ بعين الاعتبار الوثائق الموجودة و لتجنب اي تكرار في الجهد. على الرغم من ذلك ، فان فحص دقيق لـمقترح "الارشادات القانونية للبوت نت" و اتفاقية الجريمة الالكترونية، تظهر ان الي حد ما يهم القانون الجنائي فإن المقترح مختلف بشكل بسيط عن الاتفاقية. واكبر نقطتي ضعف في الاتفاقية من وجهة نظر الاتحاد الأوروبي هما عدم فعالية نقاط الاتصال لـ 24/7 و حقيقة ان الاتفاقية لا تواجه بشكل خاص الهجمات ذات النطاق الكبير. و لذلك تم تقديم معايير لإزالة هذا القصور في المقترح.

كما ذكر في بند 35، من اتفاقية بودابست يجب على كل الاعضاء ان يقوموا بتعيين نقطة تواصل والتي يجب ان تكون متاحة على مدى 24 ساعة ولمدة سبع ايام في الاسبوع ، والتي ستشكل معا شبكة 24/7 . ولكنها لا تضع اي الزامات نحو الخطوات المتبعة في حالة الحاجة الى الحصول على المساعدة. وفي المقابل، فان مقترح الاتحاد الأوروبي يتطلب ان يتم معالجة الطلبات العاجلة في خلال ثمان ساعات، على الرغم من ان الرد على الطلب قد يكون بالسلب. وثاني أكبر اختلاف تم ملاحظته بين مقترح التعليمات Botnet واتفاقية بودابست هو حقيقة ان الاتحاد الأوروبي سيقوم بوصف عقوبات ملموسة لجميع المخالفات، بينما الاتفاقية تصف العقوبات بالفعالة و المناسبة والرادعة و التي تشمل على ولكن ليس بالضرورة الحرمان من الحرية.

وبالإضافة الى ما تم ذكره انفا، فان من منظور الاتحاد الاوروبي ان تعليمات Botnet سيقدم ميزة اخرى وهو ان الدول التسع التي رفضت التصديق على اتفاقية الجريمة الالكترونية سيكونون ملزمين بتعديل تشريعاتهم حينما تصبح التعليمات حيز التنفيذ. و بما ان التعليمات تحتوي على جميع عناصر القانون الثابتة في الاتفاقية واكثر فان الهدف من توحيد تشريع الاتحاد الاوربي سيتم تحقيقه. وعلى الرغم من الاتحاد الاوروبي قد اختار ان يستغل سلطة التشريع التي يمتلكها، فان بالنسبة لباقي العالم فان اتفاقية الجريمة الالكترونية لم تفقد قيمتها واهميتها. و على الرغم من كونها قد تم صياغتها قبل عقد من الزمن، فإنها استمرت بالبقاء كأداة فعالة وأكثر سلطة في محاربة الجريمة الالكترونية، و الانضمام اليها يجب ان يكون على اجندة جميع الدول التي لم تقم بذلك ، وذلك للنجاح بملاحقة الجريمة الالكترونية الدولية.

لقد قام كلا من استونيا والمانيا بالتوقيع والمصادقة على اتفاقية الجريمة الالكترونية. بالإضافة، فان تشريعاتهم متجانسة الى حد كبير فيما يتعلق بالقوانين والتي تم توحيدها على مستوى الاتحاد الاوروبي مثل الاتصالات الالكترونية و التجارة الالكترونية و حماية البيانات الشخصية. و كيف ان الاحكام المنصوص عليها في اتفاقية الجريمة الالكترونية و تشريع الاتحاد الاوروبي تم نقلهم الى القوانين الخاصة بالأنظمة المحلية و كيف تم تفسيرهم في سياق مواجهة Botnet كما هو موضح بالأسفل.

**فيما يتعلق بتطبيقات وحدود القوانين الحالية - مكافحة البوت نت**

**1- مراقبة سجلات حركة مرور البيانات والحزم على الانترنت**

إذا كان جهاز حاسوب او شبكة من الحواسيب مصابة او يشتبه بإصابتها بأحد برامج البوت نت، فإن أولى الخطوات المنطقية يجب ان تكون بالفحص والمراقبة والتحليل لحركة مرور البيانات والحزم بجانب استخدام برنامج مكافح للفيروسات للكشف عن هذا البوت نت وتمييزه. على الرغم من إتباع هذا الأسلوب فإنه يعتبر غير فعال للكشف عن ماهية وسلوك هذا البوت نت من أجل اتخاذ الاجراءات الإضافية اللازمة لتخلص من البوت نت او أزالته بالكامل. ويستخدم عادة هذا الاسلوب في الشركات التي تستخدم بشكل أساسي شبكة الانترنت في تواصلها ويستخدم ايضا في الشركات المقدمة لخدمات الإنترنت.

في بادئ الأمر من المهم ان نلاحظ أنه يجب اجراء تمييز فيما يتعلق بالكيان الذي يراقب حركة مرور البيانات على الانترنت، فيما يتعلق بهذا الخصوص فإن بعضا من القضايا القانونية المختلفة قد تنشأ، ويرجع نشوء هذه القضايا في معظم الاحيان الي التفويض الذي يتم اعطاءه لكل كيان. بشكل عام، إن العمل الفني الروتيني الغير ضار لفحص حزم وحركة مرور البيانات محاط بعدد من الاهتمامات القانونية، أبرزها تلك المتعلقة بخصوصية الاتصال وحماية البيانات الشخصية والمراقبة الغير مصرح بها.

* **من منظور ارتكاب جنحة جنائية**

فيما يتعلق بارتكاب جنحة جنائية، فيجب ان يأخذ جانب واحد في الاعتبار عند تحليل مدى تطبيق معايير التعامل مع الجرائم الإلكترونية، وهو أن معظم الأحكام الواردة في قانون العقوبات الاستونية دخلت حيز التنفيذ فقط عام 2008، في حين أن المانيا وضعت اول قانون جنائي يتعلق بالجرائم الإلكترونية حيز التنفيذ عام 1986[[39]](#footnote-39) وكان آخرها في عام 2007 بموجب قانون العقوبات الحادي والأربعين لمكافحة جرائم الحاسوب[[40]](#footnote-40). لهذا السبب الإدانات في استونيا محدودة وأكثر التحليلات المتعلق بهذا الخصوص ليست سوى نظرية وليست مدعومة بالممارسات القضائية الكافية. وبالرغم من ذلك، إن مراقبة حركة مرور البيانات والحزم قد تقع تحت بند الجرائم التقليدية، مثل جرائم المراقبة الغير مصرح بها. فإذا كان شخص في إستونيا يراقب حركة مرور البيانات بهدف مكافحة البوت نت، فإن الخطر الرئيسي يمكن في حقيقة أن مثل هذه المراقبة يمكن أن تعتبر مراقبة غير قانونية وفقاً للأحكام المتعلقة بالقانون الجنائي من قانون العقوبات الأستونى.

***§ 137 من قانون العقوبات الاستوني، المراقبة الغير المصرح بها:***

1. *"إي شخص ينخرط بإعمال مراقبة بهدف جمع معلومات شخصية بدون حق قانوني، يعاقب بغرامة مالية أو بالسجن لمدة 3 سنوات".[[41]](#footnote-41)*

في حين أن هذه الأحكام تتعلق فقط بالجمع المتعمد للبيانات الشخصية لفرد معين[[42]](#footnote-42)، حيث أن قانون العقوبات §137 لم يوضع في البداية للأمور المتعلقة بالأنشطة الإلكترونية وإنما كان الاستخدام الرئيسي لهذه الأحكام هو التجسس على احد ما على ارض الواقع وليس إلكترونياً، ومن الممكن أن توسيع نطاق هذه الأحكام لتتضمن الأنشطة الإلكترونية أيضا. وفيما يتعلق بمضمون البيانات الشخصية فأننا نعني أي بيانات تخص عائلة شخص أو أصله أو اتصالاته أو العادات الخاصة به أو حقوق ملكيته أو التزاماته أو معتقداته الدينية الخ، على سبيل المثال يمكن لهذه المعايير أن تتحقق في حال قلنا أن الهدف من تحليل حركة مرور البيانات على الشبكة هو معرفة عادات القرصنة الخاصة بالمهاجمين خارج نطاق الإجراءات الجنائية الرسمية للتحقيق وبدون الحصول على الإذن المناسب للقيام بإجراء أنشطة المراقبة.

واستنادا إلى النظرية العامة للقانون الجنائي، فأن الغرض من تحليل البيانات يجب ان يكون له علاقة مع الجوانب الفنية لمواجهة botnet ككل وليس لجمع معلومات عن Botnet واحد بعينه، حيث لا يمكن تطبيق أحكام المراقبة الغير مصرح بها في تلك الحالة. ومع ذلك من الممكن ان يكون ذلك منطلقا لتحميل المسؤولية للأشخاص الذين يقومون بجنحة المراقبة الغير مصرح بها والتي تحدد أبعادها خلال الممارسات والتطبيق القضائي.

أيضا، كما ذَكر أعلاه، فإن التحليل القانوني قد يقود إلى نتائج مختلفة، اعتمادا على الشخص أو السلطة التي تقوم بعملية المراقبة. هنا يجب التميز ما إذا كان يتم استخدام هذه العملية بواسطة مالك الحاسوب الفعلي المتصل بشبكة بوت نت (على سبيل المثال شخص عادي أو مقدم خدمات)، أو ما إذا كان يتم استخدام هذه العملية بواسطة طرف ثالث (على سبيل المثال باحث أو فريق الاستجابة لطوارئ الحاسوب أو مزود خدمة الانترنت.) حيث أن الفرق الجوهري يكمن في مفهوم التسجيل أو التصنت على الاتصالات (بغض النظر عما إذا كانت مشفرة أم لا)[[43]](#footnote-43) ولا يمكن اعتبار طرف مسئول عن الاتصالات كجهة غير مصرح لها بالمراقبة في ضوء القانون الجنائي. ووفقاً لحكم المحكمة العليا الإستونية، لا يجوز للشخص التصنت أو تسجيل المكالمات الهاتفية الخاصة به بطريقة سرية أو مخفية، كما أيضا يجب على الطرف الآخر أن يأخذ في الحسبان احتمالية أن يتم الكشف عن هذه الاتصالات.[[44]](#footnote-44) وينطبق المبدأ ذاته بغض النظر عن قناة الاتصالات المستخدمة. بالإضافة إلى ذلك، إذا تضمن خلال عملية فحص الحزم الكشف عن محتوى الاتصالات، فإن ذلك ينتهك حق الخصوصية في الاتصالات على النحو المبين في البند 156§ من قانون العقوبات الإستونية.

***156 § انتهاك سرية رسالة***

(1) يعاقب على انتهاك سرية رسالة واردة من بريد إلكتروني أو وسائل اتصال أخرى بغرامة مالية.

المقصود بكلمة "رسالة – محتوي الرسالة الالكترونية" في هذا القسم هو محتوى البيانات فقط وليست حركة مرور البيانات.[[45]](#footnote-45) لذلك، إذا لم يتم الكشف عن محتوى بيانات أي رسالة وتم فقط تحليل حركة مرور البيانات، فإن القسم المشار إليه بشأن انتهاك السرية لا يُطبق.

يفتقر القانون الألماني لحكم مماثل للمادة 137§ من قانون العقوبات الإستونية. فإن مراقبة شخص من قبل شخص آخر مجهول جريمة إذا بلغ الأمر مستوى التعقب على سبيل المثال بواسطة إنشاء اتصال بأي وسيلة من الاتصالات (المادة§ 238 (1) رقم (2) من قانون العقوبات الألماني). حيث لا يَظهر لحكم معاقبة التعقب أهمية في سياق فحص الحزم و حركة مرور البيانات، حيث إن مثل هذه الإجراءات بالتأكيد لن تمثل انتهاكا جسيماً لحرية العمل و/أو لقرار الشخص المتضرر، كما هو مطلوب من قبل المادة§ 238[[46]](#footnote-46). ومع ذلك، يمكن أن يُعاقب على مراقبة حزم البيانات وحركة مرورها إذا كان ذلك يشكل انتهاكا لسرية الاتصالات السلكية واللاسلكية[[47]](#footnote-47) (المادة § 206 من قانون العقوبات الألماني، والمادة §88 من قانون الاتصالات، والمادة § 7 (2) من قانون تليميديا)، أو الحصول الغير قانوني للبيانات (المادة § أ202 من قانون العقوبات الألماني) أو الاعتراض الغير قانوني للبيانات (المادة § ب202 من قانون العقوبات الألماني).

ينطبق حظر انتهاك السرية البريدية أو الاتصالات السلكية واللاسلكية بمقتضي المادة 206 § من قانون العقوبات الألماني وفقاً للحقائق والمعلومات التي تنتج أثناء عملية الاتصال أو نقل البيانات.[[48]](#footnote-48) ، ولا تحمي الأحكام الحقائق[[49]](#footnote-49) أو محتوى الاتصالات فقط بل تحمي أيضا الظروف المباشرة لعملية الاتصالات (الفقرة الفرعية 5 الجملة 2). ويتم إخفاء حتى الظروف المباشرة لعملية اتصال غير ناجحة بموجب خصوصية الاتصالات (الفقرة الفرعية 5 الجملة 3).[[50]](#footnote-50) ، وتتألف "الظروف المباشرة" لعملية الاتصال، على سبيل المثال، من نقطة نهاية الاتصال ووقت جلسة الانترنت وطريقة الاتصال ومحاولاته وتخضع جميعها للحظر.[[51]](#footnote-51) ، والاهم من ذلك انه أيضا يتم إخفاء عناوين الشبكة (IP) بموجب خصوصية الاتصالات. [[52]](#footnote-52)، وبما أن فحص حركة مرور البيانات وحزم الانترنت سوف تتضمن بيانات تعود إلى عملية الاتصالات بين خادم التحكم والسيطرة (C&C) على شبكة (الذي يتحكم بجميع الاجهزة المصابة بالبوت نت الخاص به لتكون تحت تصرف المعتدي) والجهاز المصاب بالبوت نت وبالتالي فإن "الظروف المباشرة" لعملية الاتصال ومنع انتهاك عملية الاتصال ستكون ذات صلة في هذا السياق.

***206 § انتهاك خصوصية البريد و الاتصالات[[53]](#footnote-53)***

(1) إن كل شخص يكشف بصورة غير قانونية عن بيانات شخص آخر بحيث تكون هذه البيانات خاضعة للخصوصية البريدية أو الاتصالات وأصبحت هذه البيانات معروفة له باعتباره مالك أو موظف يعمل في مؤسسة تعمل في مجال تقديم الخدمات البريدية أو الاتصالات، سيعاقب إما بالسجن لمدة لا تزيد عن 5 سنوات أو بغرامة مالية.

(2) أي شخص بصفته مالك أو موظف في مؤسسة يقوم بالتالي ذكره بصورة غير قانونية يطبق عليه البند (1) كما هو مبين أعلاه

1- أن يقوم بفتح بريد مختوم في عهدت مؤسسة موكلة بتسليمه لكسب معرفة محتواه دون تمزيق الختم وباستخدام وسائل تقنية

-2 أن يعيق إرسال بريد في عهدت مؤسسة موكلة بتسليمه

أو

3- كل من يسمح أو يشجع لعمل مثل هذه الأعمال المشار لها في البند (1) أو المشار لها في رقم 1 أو 2 أعلاه، سيطبق عليه نفس العقوبة.

(3) الأقسام الفرعية (1) و (2) أعلاه تطبق أيضاً على الأشخاص الذين

1- يقومون بمهام إشراف على مؤسسة كما هو مشار في الفقرة الفرعية (1) أعلاه

2- أشخاص موكلين من قبل المؤسسة أو من قبل تفويضها، لتقديم الخدمات البريدية أو الاتصالات، أو

3- أشخاص موكلين بإنشاء مرافق تخدم العمل أو تتعلق بتأديته في مثل هذه المؤسسة.

(4) أي شخص مخول له أو غير مخول له يكشف بصورة غير قانونية عن بيانات شخص آخر وأصبحت هذه البيانات معروفة له باعتباره موظف عمومي خارج الخدمات البريدية أو الاتصالات سيعاقب إما بالسجن لمدة لا تزيد عن سنتين أو بغرامة مالية.

(5) تخضع الظروف المباشرة للعمليات البريدية المتعلقة بأشخاص معينين وكذلك محتوى البريد للخصوصية البريدية. يخضع محتوى الاتصالات وظروفه المباشرة للخصوصية البريدية وخاصة حقيقة ما إذا كان شخص ما قد شارك أو يشارك في عملية الاتصالات. وتمتد أيضاً خصوصية الاتصالات لتطال الظروف المباشرة لمحاولات إجراء اتصال باءت بالفشل.

**وبالتالي، فإن جريمة ارتكاب انتهاك لخصوصية الاتصالات تتحقق، إذ:**

- كان موظف أو مالك لشركة مزودة لخدمات الاتصالات (مزودة خدمة الانترنت أو شركة تقدم خدمات اتصال لموظفيها، وتسمح بالاستخدام الخاص للإنترنت)،

- المشرف على مثل هذه الشركة،

- مقاول فرعي يقوم بتزويد خدمات الاتصالات، أو

- مقاول فرعي يقوم بإنشاء مرافق تخدم عملية تقديم خدمات الاتصالات أو تتعلق بتأديتها،

- موظف عمومي خارج الخدمة البريدية أو الاتصالات سواء أكان التعدي على الخصوصية البريدية والاتصالات مخول له أو غير مخول.[[54]](#footnote-54)

أو الكشف عن محتوى عملية الاتصالات لشخص آخر بصورة غير قانونية.[[55]](#footnote-55) غير أن مجرد حفظ البيانات المقرون بإتباع بروتوكول معين وبدون الكشف عن محتواها لأي شخص فإن ذلك لا ينتهك المادة § 206.[[56]](#footnote-56) ، مع الاعتبار أن الكشف الغير قانوني يمكن أن يحدث حتى داخل نفس الشركة، إذا كان الشخص الذي يتلقى البيانات المحمية لا يحتاج لها وفقاً لمهام أو مسؤوليات أو هيكلية العمل المتعلقة بتزويد خدمة الاتصالات.[[57]](#footnote-57)

قسم المادة 88 من قانون الاتصالات الألماني والمادة § 7 (2) من قانون تليميديا يَرَيَانِ ضرورة امتثال مقدمي خدمات الاتصال الإلكترونية لـ "***لخصوصية الاتصالات***" كالتزام قانوني. ومن المثير للاهتمام، ووفقاً لتعريف (المادة § 3 البند 6 فرع أ) ووفقاً (للبند 10 من قانون الاتصالات) و(المادة § 2 البند 1 من قانون تليميديا)، فإن كل شركة تسمح لموظفيها بالاستخدام الخاص لأجهزة الإنترنت الخاصة بالشركة تعتبر شركة مزودة لخدمات الإنترنت.[[58]](#footnote-58)، وفي سياق متصل إن خصوصية الاتصالات تشير للظروف المباشرة للاتصال مثل وقت جلسة الانترنت ونهايتها كاستخدام خاص للإنترنت أو كاستخدام يتعلق بالاتصالات التجارية في حال إذا كان من غير الممكن فصلهم عن الاتصالات الخاصة.

***المادة § 7 من قانون تليميديا. المبادئ العامة[[59]](#footnote-59)***

مقدمي خدمات الاتصالات مسئولين قانونياً بمقتضى القوانين المعمول بها فيما يتعلق بالمعلومات التي يقدمونها للاستخدام. (1)  
(2) بمقتضى المادة § 10 والمادة § 8، مقدمي خدمات الاتصالات ليسوا مضطرون لمراقبة أو تخزين البيانات التي يعالجونها وليسوا مضطرون أيضا للبحث عن الظروف التي من شأنها أن تشير إلى وجود نشاط غير قانوني. حيث في حال بقيت هذه القوانين دون تغير فإن هذا الاضطرار يحظر و يمنع أيضاً استخدام هذه البيانات عملاً بمقتضى المادة § 8 و المادة § 10، حتى ولو كان هناك عدم وجود للمسؤولية من طرف مزودي خدمات الاتصالات. فبمقتضى المادة § 88 من قانون الاتصالات، يجب أن تأخذ خصوصية وسرية الاتصالات بالحسبان.

***المادة 88 من قانون الاتصالات. خصوصية الاتصالات***

1. ينبغي أن يخضع محتوى ظروف الاتصالات وتفاصيلها، لاسيما إذا كان شخص منخرط في أنشطة الاتصالات أو لا، فينبغي على هذا الشخص أن يخضع لخصوصية الاتصالات أيضاً. وينبغي على الخصوصية أيضاً أن تشمل تفاصيل أي محاولات اتصال غير ناجحة تحيط بالظروف.
2. يجب على كل مزود خدمات أن يلتزم بالحفاظ على خصوصية الاتصالات. حيث يسري هذا الالتزام بالحفاظ على الخصوصية بعد نهاية أي نشاط جرى خلاله التعهد بالالتزام.
3. يجب على جميع الأشخاص ذوي الالتزامات أن يمتنعوا عن تقديم الخدمات لأنفسهم أو لأطراف أخرى وفقا للفقرة الفرعية (2)، على النقيض من ذلك لا تعارض في استخدام أي معلومات تخص محتوى أو تفاصيل ظروف الاتصال والتي بدورها تعتبر ضرورية لغايات الإعلان التجاري الخاص بخدمات الاتصالات الخاصة بهم، وبما في ذلك أيضا توفير الحماية اللازمة لأنظمتهم التقنية. إن معرفة الحقائق الخاضعة لخصوصية الاتصالات يمكن أن تستخدم فقط للغرض المشار إليه في الحكم (1).

إن استخدام هذه المعرفة لأغراض أخرى، خصوصاً إرسالها إلى أطراف أخرى، مسموح فقط بالقدر المنصوص عليه بشأن هذا الجانب أو بالقدر الذي ينص عليه أي حكم قانوني يتعلق بوضوح بقضية أنشطة الاتصالات. ويجب أن تكون الأولوية للقسم مادة 138 من قانون العقوبات للحكم بشأن هذا الأمر.

إن خصوصية الاتصالات تتضمن حظر الكشف عن البيانات المحمية للآخرين، كما هو مبين في المادة § 7 (2) من قانون تليميديا و أيضا في المادة § 88 (3) من قانون الاتصالات، على سبيل المثال كالكشف عن هذه البيانات لباحث خاص، أو حتى كشفها لأشخاص يعملون بنفس الشركة التي توفير خدمات الاتصال (يستثنى من ذلك الأغراض المتعلقة بالفواتير). ومن الجدير بالذكر أنه وفقاً للمحكمة الإدارية "هيسنHessen " إن نصوص خصوصية الاتصالات تسري فقط أثناء عملية الاتصالات حيث أن بعد نهاية عملية الاتصالات أي بيانات يتم حفظها سوف تكون محمية من قبل نصوص وأحكام خصوصية البيانات[[60]](#footnote-60).

وعلى الرغم من ذلك، ووفقاً للمادة 88 (3) من قانون الاتصالات فإن الحظر عن الكشف للبيانات المحمية للآخرين لا ينطبق صراحة على المعلومات الضرورية لتوفير الخدمات أو لحماية الأنظمة التقنية الخاصة بمزودي الخدمات. وبناء على ذلك، المادة § 100 من قانون الاتصالات تسمح لمزود خدمة الاتصالات بجمع واستخدام بيانات العملاء من أجل المعرفة أو الحد أو حل مشكلة أو خطأ في أنظمة الاتصالات. مع الوضع بالاعتبار مبدأ "وحدة النظام القضائي"، حيث إن النصوص والبنود تكون ذات صلة في حال تقييم معيار الكشف "الغير قانوني" للبيانات كما هو مطلوب في المادة § 206 (1) من قانون العقوبات الألماني.[[61]](#footnote-61) ، لذلك عندما تطبق المادة § 100 من قانون الاتصالات الألمانية فإن استخدام وتحليل البيانات للأغراض المبينة أعلاه (من أجل المعرفة أو الحد أو حل مشكلة أو خطأ في أنظمة الاتصالات) لا يؤدي إلى انتهاك الخصوصية الاتصال أو البريد (المادة § 206 من قانون العقوبات الألماني، والمادة § 88 من قانون الاتصالات الألماني). حيث أن الخلل أو الخطأ في نظام الاتصالات يمكن أن يحدث نتيجة، على سبيل المثال، عندما يتم استخدام البوت نت لغرض شن هجمات باستخدام طريقة رفض الخدمة (DDOS)[[62]](#footnote-62).

***المادة*** ***§ 100 الأعطال في أنظمة الاتصالات و الاحتيال في استخدام خدمات الاتصال***

1. قد يحتاج مزود الخدمة لجمع بيانات الزبائن أو المشتركين أو المستخدمين حين يكون ذلك مطلوباً، ليكشف عن أو يحل مشكلة أو يصلح عطلاً في أنظمة الاتصالات.
2. يسمح لمشغل نظام الاتصالات و ممثله المخول بالدخول على اتصال معين، في حال طرأ تغيرات على نظام تطبيقات الاتصال أو لغرض التحديد والتعرف على مكان الأعطال في الشبكة، في حال كان هذا الدخول مطلوباً من الناحية العملية فيجب أن يكون الدخول على هذا الاتصال مقروناً بإخطار شفوي وصريح للأطراف المعنية.
3. قد يحتاج مزود الخدمة لجمع بيانات الزبائن أو المشتركين حين يكون ذلك مطلوباً، للكشف عن أو وضع حد للاستخدام الخفي للخدمات و الاستخدامات الغير قانونية الأخرى للخدمات و لشبكات الاتصالات وفي حال كان هنالك وجود لمثل هذا الاستخدام يجب أن تسجل التفاصيل كتابتاً بالإشارة لهذا الخصوص. وللغرض المشار إليه في الحكم 1 قد يحتاج مزود الخدمة لاستخدام بيانات مجموعة مسبقاً لتحديد إجمالي البيانات التي لا يزيد عمرها عن 6 شهور، حيث يمكن لتلك البيانات المتعلقة بشبكة الاتصالات أن تدل على أن هناك استخدام غير قانوني حدث لشبكات الاتصالات و الخدمات. حيث يمكن لمزود الخدمة أن ينشأ ملف بيانات مستعار بواسطة استخدام بيانات الزبون المجموعة بمقتضى الحكم 1 والذي بدوره يوفر معلومات عن الرسوم والعائدات المجبية من المشتركين الأفراد والذي يعتبر أيضا ضابطاً مناسباً لحالات الاحتيال، والذي يسمح بجمع البيانات في حال كان هناك أساسات تدل على أن هناك استخدام سري للخدمات، حيث إن وجد هذا الاستخدام فيجب أن تمحى جميع البيانات المتعلقة بالاتصالات الأخرى والتي ليس له علاقة بدون تأخير لا مبرر له. ويجب أن يتم إشعار الهيئة التنظيمية ومفوض حماية البيانات الفدرالي عن أي تعديل أو إدخال يطرأ على القضية وفقاً للحكم 1.
4. ومع مراعاة الشروط المشار إليها في البند (3) الحكم 1، قد يقوم مزود الخدمات في لحظة معينة بجمع و استخدام البيانات بالقدر الذي لا غنى عنه لتوضيح ووضع حد للأعمال الموضحة هناك. حيث أن جمع واستخدام أي محتوى آخر للاتصالات الأخرى غير مسموح به. ويجب أن يتم إشعار الهيئة التنظيمية بالإجراءات المتخذة وفقاً للحكم 1. ويجب أن يتم تحذير الأطراف المعنية في اقرب وقت ممكن لتسوية أمورها قبل أن تقع في الخطر.

يُسمح لمزودي خدمات الانترنت بجمع وتحليل عناوين البروتوكولات الخاصة بالمستخدمين لمدة تصل إلى سبعة أيام على أساسات عامة، من أجل كشف أو تحديد أو إصلاح عيب أو عطل في الشبكة و أنظمة الاتصالات الخاصة بهم.[[63]](#footnote-63) وذلك وفقاً لقرار المحكمة الاتحادية الألمانية العليا عام 2011، المادة § 100 (1) من قانون الاتصالات، ويؤكد قرار المحكمة أن إرسال رسائل البريد الخبيثة (Spam)، أو نشر البرمجيات الخبيثة (البوت نت والفيروسات وغيرها من البرمجيات الخبيثة) أو إساءة استخدام أنظمة الحواسيب باستخدامها كمنصة لهجمات رفض الخدمة DDos يمكن أن يسبب أعطال وأخطاء كبيرة في أنظمة الاتصالات.[[64]](#footnote-64) ، لذلك إن عملية جمع ومعالجة حركة مرور البيانات (بما في ذلك عناوين بروتوكولات الإنترنت) محمية بموجب الإذن الممنوح من قبل قانون الاتصالات § 100 (1) لأغراض الكشف والقضاء على منبع الرسائل الخبيثة و البرمجيات الخبيثة و هجمات رفض الخدمة DDos. وفي حال تم الكشف خلال سبعة أيام عن الأسباب المحددة التي تسبب الأخطاء والأعطال، فإن مزود خدمة الانترنت مسموح له بحفظ وتحليل البيانات المناسبة لفترة أطول من سبعة أيام، أو بالفترة الكافية للقضاء على الأسباب المؤدية لمثل هذه الأعطال والأخطاء[[65]](#footnote-65).

***§ أ 202. التجسس على البيانات***

1. أي شخص يحصل بشكل غير قانوني على بيانات لا تخصه وكانت هذه البيانات محمية من الوصول غير المصرح به أو أي شخص يتحايل على نظام الحماية، يعاقب أما بالحبس لمدة لا تزيد عن 3 سنوات أو بغرامة مالية.
2. ضمن مغزى البند (1) أعلاه، فيجب أن تحفظ البيانات او ترسل إلكترونيا أو مغناطيسياً أو بأي طريقة أخرى يصعب اختراقها.

ومع ذلك يجب الأخذ بالحسبان حتى ولو كانت البيانات والحزم التي يتم مراقبتها غير محمية فإن القانون يعاقب أيضا على هذه الفعلة باعتبارها كاعتراض غير قانوني للبيانات وفقاً للمادة (§ ب 202) من قانون العقوبات الألماني، والتابع للمادة المذكورة سابقاً (§ أ 202)[[66]](#footnote-66).

***§ ب 202. اعتراض البيانات***

أي شخص يستخدم وسائل تقنية ليعترض بيانات لا تخصه أو تخص أي شخص أخر وبشكل غير قانوني (§أ 202 (2))، وسواء تم اعتراض هذه البيانات من منشأة خاصة بمعالجة البيانات او من خلال البث الكهرومغناطيسي الخاص بهذه المنشأة، فإنه يعاقب إما بالسجن لمدة لا تزيد عن سنتين او بغرامة مالية، ما لم يكن عقاب هذه الجنحة أشد بمقتضى أحكام أخرى.

إن المصلحة التي يهدف القانون لحمايتها هي "المصلحة الرسمية" المتعلقة بالأشخاص المخول لهم بحماية خصوصية عملية الاتصالات، والتي ينبغي عليها ان لا تلتقي بالمصالح الشخصية للأشخاص المعنيين.[[67]](#footnote-67) بيانات الاتصالات القديمة وعمليات نقل البيانات المكتملة ليست محمية من قبل المادة.[[68]](#footnote-68) وهذا يعني ان الهدف من هذا الحكم هو تجريم اعتراض البيانات الخاصة بالشبكات الغير محمية المتعلقة بمعالجة "البيانات الخاصة". حيث يشير مصطلح معالجة "البيانات الخاصة" الى جميع البيانات المتعلقة برسائل البريد الإلكتروني أو المحادثات الإلكترونية أو اتصالات الشبكات الخاصة الافتراضية او المحادثات الصوتية عبر الانترنت.[[69]](#footnote-69) حيث أن اعتراض مثل هذه البيانات يعاقب عليه القانون، إلا في حال كانت هذه البيانات تخص الشخص المعترض، على عكس اعتراض معالجة البيانات "العامة"، فإن القانون لا يعاقب عليها لأنها مخصصة لعامة الناس. إن عدم وجود تشفير للبيانات خلال عملية الإرسال لا يعني ان هذه البيانات يقصد بها ان تكون متاحة لعامة الناس.[[70]](#footnote-70) بطبيعة الحال إن اعتراض البيانات من قبل المسئولين او الموظفين في شركة خاصة بتزويد خدمات الانترنت وكان هذا الاعتراض ضرورياً لضمان سير عملية الخدمة التي يقدمونها فإن ذلك لا ينتهك القانون، لأن هذه البيانات بالطبيعة الحال تخصهم باعتبارهم مزودين لخدمة الانترنت. وبالتالي فإنه يمكن لمالكي وموظفين شركة مزودة لخدمات الانترنت او فريق الاستجابة لطوارئ الحاسوب الخاص بالشركةCERT أن يقوموا فقط بإجراء فحص وتحليل مقنن لحزم وبيانات الانترنت من اجل تحديد وكشف (البوت نت) مع الوضع في الحسبان عدم ارتكاب انتهاك خلال عملية الفحص هذه، حيث إنه من الضروري عليهم التعرف على الأخطاء والتشويش في أنظمة الاتصالات الخاصة بهم وإصلاحها. في حين أن مثل هذا التشويش والأخطاء تحدث نتيجة لنشاطات (البوت نت) والذي بدوره يستخدم أجهزة المستخدمين من أجل شن هجمات رفض الخدمة مما يخلق مجال كبير لمرور البيانات الخبيثة. مع الاعتبار أنه يجب عليهم حذف البيانات التي تم جمعها بشكل مباشر بعد الانتهاء من تحديد مصدر الأخطاء او التشويش أو في حال تم حل المشكلة. في حين انه لا يمكن لهم بكل تأكيد ان يمروا من تحت أعين باحث مستقل بدون ان يكونوا مجهولي الهوية، لأن هذا الأمر من شأنه أن يشكل جريمة انتهاك لخصوصية الاتصال. حيث إن الباحث المستقل الذي يراقب حركة مرور البيانات والحزم على الانترنت عرضه لارتكاب جنحة الاعتراض الغير مصرح به للبيانات، إذا قام بجمع بيانات متعلقة بجلسات انترنت "خاصة"، وذلك عملاً بمقتضى مضمون الحكم المتعلق بهذا الأمر.

إن موافقة المشترك على جمع وتخزين بياناته تلغي المسؤولية الجنائية عن عاتق الأشخاص الذين يقومون بعملية المراقبة في جميع الأحوال، وبالرغم من ذلك، تجدر الإشارة الى انه بناء على مسألة مراعاة حماية المشترك، فإن القانون يضع ويحدد معايير معقدة بخصوص موافقة المشترك بجمع وتخزين بياناته من قبل مزودي خدمات الاتصالات، وفي الوقت نفسه يلزم مزودي الخدمات على اعطاء معلومات مفصلة عن نوع البيانات التي سيتم جمعها وتخزينها بالإضافة الى الهدف من وراء جمع وتخزين مثل هذه البيانات. إن موضوع الموافقة على جمع وتخزين البيانات والحزم يصبح ذو صلة في سياق المادة § 206 من قانون العقوبات الألماني إذا أعطيت الموافقة لمثل هذا الجمع والتخزين من قبل جميع المشتركين في خدمة الاتصالات 104، وفي أغلب الأحيان لن يتم اعطاء موافقة من الجميع خصوصاً الطرف الذي يسيطر على (البوت نت)، والذي يقوم بإنشاء اتصال بين خادم التحكم والسيطرة ((C&C والحاسوب الذي يحتوي (المصاب) على البوت نت. في حين لو كانت مراقبة حركة البيانات والحزم تحدث داخل الشركة ذاتها، فإن القيام بمثل هذه المراقبة يعتبر "كمراقبة فنية" والتي بدورها تتطلب موافقة من مجلس الشركة، إن وجد (طالع المادة § 87 الفقرة 1 رقم 6 من قانون دستور مجلس الأعمال).

ومن ناحية أخرى، إن مراقبة البيانات او الحزم او الكشف عنهما لا ينتهك القانون إذا كان قرار المراقبة والكشف صادر من المحكمة، وذلك يتم تطبيقه في إطار السلطات التنفيذية المخولة او من خلال وكالات التحقيق الخاصة بالدولة وذلك بمقتضي المادة (§ أ 100) من القانون الإجراءات الجنائية الألمانية أو من باب اتخاذ التدابير اللازمة من قبل السلطات الشرطية المخولة وفقاً للستة عشر قانوناً مختلفاً في الولايات الألمانية [[71]](#footnote-71) او وفقاً للمادة (§ ك 20) من قانون مكتب الشرطة الجنائية الفدرالي. أما بالنسبة لعمليات التحقيق او الإجراءات القضائية الأخرى التي تجريها وكالات الدولة التنفيذية، فإنه يجب تقديم دليل مادي وملموس عند الاشتباه بشخص ما يقوم بارتكاب جنحة جنائية.

في النهاية، فإنه يمكن الجزم بان "التحقيقات" المتعلقة بالكشف عن أنشطة البوت نت والتي بدورها تشمل جمع بيانات عن "الظروف المباشرة" لعملية اتصال هي بالأساس مسؤولية السلطات التنفيذية. في المقابل ووفقاً للمادة ( § 7 (2)) من قانون تليميديا الخاص بمزودي خدمات الاتصالات فإنه ليس من مسؤولية مزودي خدمات الاتصالات ان يقوموا بمراقبة المعلومات المعالجة او المخزنة او ان يقوموا بالبحث عن معلومات يمكن من شأنها ان تشير الي وجود أنشطة غير قانونية.[[72]](#footnote-72) وهذا يتضمن أيضا البحث عن مخاطر غير معلومة بعد، وإذا وجد حتى أثر لنشاط غير قانوني، فإنه يمكن ان تنشأ مطالب بالتوقف والكف عن مراقبة هذا النشاط حتى وإن كانت مراقبة هذا النشاط كإجراء وقائي، حيث انه أيضا يجب على أي شخص عادي يقوم بمراقبة للبيانات والحزم - لأغراض غير متعلقة بإصلاح عطل او تشويش في شبكة الاتصال- أن ينصاع للقوانين التي تحمي خصوصية عملية الاتصالات. وبالتالي فإنه يجوز فقط البحث عن أنشطة البوت نت باستخدام بيانات مجهولة المصدر، (أي عدم تضمين عناوين بروتوكولات الانترنت والبيانات المحمية بموجب خصوصية الاتصالات خلال عملية الفحص) وكل ذلك يجب ان يخضع لأحكام القانون الجنائي.

**ملاحظات ختامية**

يبقي البوت نت يشكل تهديداً لمستخدمين شبكة الانترنت، لذلك يتم استخدام طرق فعالة وجديدة بين الحين والأخر لكبح استخدامه و انتشاره. وحيث تعتبر عمليات الاستيلاء او الإزالة المباشرة للبوت نت من انجح الطرق المستخدمة لمكافحته. ومع ذلك فإن يجب ان يتم تقيم تقنيات مكافحة البوت نت بعناية لمعرفة مدى قانونيتها. في حين يبقى احتمال نشوء قيود على الإجراءات المضادة لمكافحة البوت نت قائماً من طرف أي مجال قانوني سواء القانون الإداري او المدني او الجنائي.

ومن جهة أخرى، إن القانون لا يكتفي بوضع قيود على سلوكيات الأشخاص فقط، وإنما يتطلب أيضا تدخل الجهات المعنية لاتخاذ إجراءات لمكافحة البوت نت في مواقف معينة، في حين ان مثل هذا الالتزام منبثق من خلفية الواجبات العامة للعمل والتصرف مهما كان، حتى ولو بدون اعطاء موضوع البوت نت اهتماما على وجه الخصوص. وبطبيعة الحال، ان مزودي خدمات الانترنت ووكالات القضاء التنفيذية هم الذين يتحملون العبء الأكبر بهذا الخصوص. على سبيل المثال لنفترض ان شبكة الاتصالات الخاصة بمزود خدمة انترنت مهددة بخطر واضح، هنا يكون واجباً على مزود خدمة الانترنت إبلاغ المستخدمين عن هذا الخطر، ويكون مطلوباً من قوى القانون التنفيذية او هيئة الادعاء ان يتخذوا الإجراءات اللازمة في حال ظهرت عناصر الجريمة. إن المسؤولية المدنية عند إبلاغ مزود خدمة الانترنت المستخدمين بالخطر الواقع تجعل الأمر صعباً على الشخص الذي يقوم باستخدام البوت نت لشن هجومه باستخدامه أجهزة المستخدمين كمنصة للهجوم. وهذا الأمر يقود الى ضرورة و أهمية تثقيف المستخدمين عن التهديدات التي تحيط بهم على الانترنت بما فيها البوت نت وإرشادهم الى استخدام الإجراءات الأمنية اللازمة لحماية بياناتهم على الانترنت.

وبالإشارة الي ما يتعلق بتطبيق حدود قوانين مكافحة البوت نت فإن تطبيق مثل هذه القوانين ما يزال محدوداً، وبالنسبة للإجراءات المتعلقة بمكافحة البوت نت المذكورة في هذا التقرير فإنها ليست مسموحة بشكل مطلق ولا محظورة من القانون، حيث ان هدف هذا التقرير في المقام الأول كان للفت انتباه القارئ لنقاط الاختلاف بين الأحكام، ويؤكد ان القرار دائماً في النهاية يترك للمحاكم لتحديد قانونية او غير قانونية الفعلة.

مقدم البحث / م. محمد أبو لمضي

ماجستير هندسة دفاع أمن المعلومات Cyber Security- جامعة تارتو و جامعة تالين للتكنولوجيا– استونيا 2014.

محاضر في كلية تكنولوجيا المعلومات/ وقسم هندسة البرمجيات - جامعة فلسطين www.up.edu.ps – مدينة الزهراء – قطاع غزة.

-شارك في تدريبات الناتو " الحصن المنيع 2014" وهو تدريب تقني محاكاة واقعي للدفاع و الهجوم واسع النطاق ومتطور على شبكة الانترنت، بإشراف فريق قانوني ، لمدة 3 ايام يشارك به النخبة من الكوادر المدنية و العسكرية من 25 دولة . 2014

- شارك في دورة "تحليل جرائم الحاسوب" لمدة 3 اسابيع . 2013 جمهورية لثوانيا

- شارك في دورة " الانظمة الامنية الحساسة" لمدة اسبوعين. 2014 ايطاليا.

m.abulamddi@up.edu.ps

m.abulamddi@gmail.com

جوال : 0597865554

العنوان : شارع الجلاء ، الشيخ رضوان – قطاع غزة.

1. هي شبكة من الحواسيب (تشمل اجهزة الهاتف الذكي) موزعة حول العالم مصابة ببرمجيات خبيثة وتصبح هذه الحواسيب خاضعة لجهات اخري، وهذه البرمجيات الخبيثة اما يكون في حالة خاملة او نشطة، و هذه الحواسيب المصابة (تكون ربما 100000 جهاز مصاب) تتلقى الاوامر من جهاز رئيسي يسمي (جهاز السيطرة والتحكم) يتحكم بها وتكون خاضعة له، وتستخدم الاجهزة المصابة لشن هجوم فعال على الخدمات الالكترونية المصرفية او انظمة البنية التحتية من دون تعقب المصدر الحقيقي للهجوم، لأنه يتم الهجوم من قبل اجهزة مصابة من حول العالم وهذه الاجهزة لأشخاص او مؤسسات لا يعلمون ما تقوم به اجهزتهم. لهذا الاتحاد الاوروبي اعطى له اهمية كبيرة في التعامل مع هذا التوع البوت نت من البرامج الخبيثة لأنه يتعلق ايضا بالخصوصية. [↑](#footnote-ref-1)
2. See, e.g., Menn, J. Fatal System Error: The Hunt for the New Crime Lords Who are Bringing Down the Internet. PublicAffairs, 2010; Villeneuve, N. KOOBFACE: Inside a Crimeware Network. November 2010. [↑](#footnote-ref-2)
3. Microsoft Security Intelligence Report, Vol. 12, July through December 2011. Available at:

   http://www.microsoft.com/security/sir/default.aspx [↑](#footnote-ref-3)
4. Shadowserver Foundation. Botnet Charts. Available at: http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts [↑](#footnote-ref-4)
5. Famous examples of botnets include Agobot (2002); Spybot, Rbot, Sinit (2003); Beagle, Bobax (2004); Rustock, ZeuS (2006); Pushdo, Storm, Cutwail, Srizbi (2007); Asprox, Kraken, Mega-D, Torpig, Conficker, McColo (2008); BredoLab, Grum, Maazben (2009); Waledac (2010); Kelihos, BlackShades (2011). [↑](#footnote-ref-5)
6. *Tikk, E., Kaska, K., Vihul*, *L*. International Cyber Incidents: Legal Considerations. CCD COE

   Publishing, Tallinn, 2010. [↑](#footnote-ref-6)
7. Council of Europe, Convention on Cybercrime. ETS no. 185. Budapest, 23.11.2001. Available at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [↑](#footnote-ref-7)
8. EU law or community law means the set of rules adopted by the European Community. Community law consists mainly of the Treaties and the instruments adopted by the institutions under the Treaties, such as Regulations and Directives. The case-law of the Court of Justice is also one of the sources of Community law. [↑](#footnote-ref-8)
9. A Commission Communication is a policy document with no mandatory authority. The Commission

   takes the initiative of publishing a Communication when it wishes to set out its own thinking on a topical issue. A Communication has no legal effect. – http://ec.europa.eu/civiljustice/glossary/glossary\_en.htm [↑](#footnote-ref-9)
10. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach. COM(2001)298, p. 3. [↑](#footnote-ref-10)
11. Although in the context of NIS the EU prefers to consider them together, they could also be viewed as two separate categories. [↑](#footnote-ref-11)
12. كما اشرنا سابقا ان Botnet حالة خاصة لأنه يتم الهجوم من اجهزة اشخاص لا يعرفون ان جهازهم الحاسوب او الموبايل مصاب ببرامج خبيثة وتستخدم لشن هجوم على احد الخدمات الالكترونية. ولهذا تصبح المسألة تتعلق بالخصوصية لهذا المستخدم في التعامل مع بياناته والملفات المستخرجة من جهازه لغرض فحصها من اجل الوصول إلى المصدر الاساسي، وكل دول من دول الاتحاد الأوروبي تتعامل مع الخصوصية بشكل صارم وعالي المستوي مما يفرض تحديات على الجهات المشاركة في التحقيقات. [↑](#footnote-ref-12)
13. Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society – “Dialogue, partnership and empowerment”. COM(2006)251, p. 4 [↑](#footnote-ref-13)
14. مدينة فنلندية، عاصمة إقليم بيركانما جنوبي البلاد [↑](#footnote-ref-14)
15. In the EU, the terms ‘cyber crime’, ‘computer crime’, ‘computer-related crime’ and ‘high tech crime’ have been used as synonyms, especially at the beginning of the previous decade. Today, however, referring to ‘cyber crime’ appears to be the prevalent practice. [↑](#footnote-ref-15)
16. The European Commission’s main function is to propose and implement Community policies adopted by

    the Council and the Parliament. It acts in the general interest of the Union with complete independence from national governments. It enjoys a quasi-exclusive right of initiative in matters where the Community method applies (matters where Member States have transferred a significant part of their responsibilities, such as the Common Agricultural Policy, the Customs Union, the internal market, the Euro, etc.), which drive European integration [↑](#footnote-ref-16)
17. eEurope 2002 An Information Society For All. Action Plan prepared by the Council and the European Commission for the Feira European Council. 19-20 June 2000. COM(2000)330, p. 10. [↑](#footnote-ref-17)
18. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime. COM(2000)890. [↑](#footnote-ref-18)
19. *Supra nota* 30, pp. 25-26. [↑](#footnote-ref-19)
20. Before the adoption of the Lisbon Treaty, under Article 34(2)(b) of the Treaty on European Union, framework decisions were used to approximate the laws of Member States similarly to directives. They were binding upon the Member States as to the result to be achieved, but left to the national authorities the choice of forms and methods. The institute of a framework decision was abolished when the Lisbon Treaty came into force. [↑](#footnote-ref-20)
21. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. [↑](#footnote-ref-21)
22. ‘Manipulating’ is a word used by the author to cover all activities listed in Article 3: ‘inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data’. [↑](#footnote-ref-22)
23. Communication from the Commission to the European Parliament, the Council, the European Economic

    and Social Committee and the Committee of the Regions on fighting spam, spyware and malicious software. COM(2006)688, p. 3. [↑](#footnote-ref-23)
24. Communication from the Commission to the European Parliament, the Council and the Committee of the

    Regions - Towards a general policy on the fight against cyber crime. COM(2007)267, p. 3. [↑](#footnote-ref-24)
25. *Supra nota* 46, p. 8. [↑](#footnote-ref-25)
26. Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems. COM(2008)448, p. 10. [↑](#footnote-ref-26)
27. Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA. COM(2010)517. [↑](#footnote-ref-27)
28. Commission Staff Working Document Impact Assessment Accompanying document to the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems, and

    repealing Council Framework Decision 2005/222/JHA. SEC(2010)1122, p. 21. [↑](#footnote-ref-28)
29. The European Economic and Social Committee is a consultative body of the EU which integrates social and economic interest groups. Its 344 members are nominated by national governments for a term of five years. The Committee’s task is to issue opinions on matters of European interest to the Council of the European Union, to the European Commission and to the European Parliament. [↑](#footnote-ref-29)
30. Opinion of the Economic and Social Committee on the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, 4 May 2011, point 1.10 [↑](#footnote-ref-30)
31. Article 35 of the Council of Europe Cybercrime Convention foresees that the Signatories shall “designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence”. [↑](#footnote-ref-31)
32. *Supra nota* 8. [↑](#footnote-ref-32)
33. Explanatory report to the Convention on Cybercrime. Chapter III, point 16. [↑](#footnote-ref-33)
34. *Supra nota* 39, p. 11. [↑](#footnote-ref-34)
35. *Supra nota* 40, p. 15. [↑](#footnote-ref-35)
36. *Supra nota* 46, p. 6. [↑](#footnote-ref-36)
37. Proposal for a Council Framework Decision on attacks against information systems. COM(2002)173, p. 8. [↑](#footnote-ref-37)
38. The Stockholm Programme – An open and secure Europe serving and protecting citizens. 2010/C 115/01, point 4.4.4. [↑](#footnote-ref-38)
39. Second Law to combat economic crime (Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG)), BGBl I, 721; with further annotations in BT-Drs. 10/318. First introduction of ‘data espionage’

    § 202a German Criminal Code and ‘data manipulation’ § 303a German Criminal Code; see Laue, in: jurisPR-StrafR, 13/2009, Anm. 2. [↑](#footnote-ref-39)
40. Criminal Law Amendment Act to combat computer crime (Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄG)), BGBl 2007 I, 1786; with further annotations in BT-Drs. 16/3656 and BT-Drs. 16/5449. [↑](#footnote-ref-40)
41. The translations of the Estonian legal acts into English are available on the website of the Estonian Ministry of Justice at http://www.just.ee/23295. [↑](#footnote-ref-41)
42. *Sootak, J., Pikamäe, P*. Karistusseadustik. Kommenteeritud väljaanne. Juura, 2009, p. 405. [↑](#footnote-ref-42)
43. The botmaster normally applies techniques to make the communication between the infected client and the C&C server not readable, e.g. by encryption. [↑](#footnote-ref-43)
44. The Supreme Court of Estonia, Criminal Chamber ruling of 26 March 2009 no. 3-1-1-5-09. [↑](#footnote-ref-44)
45. Although according to Estonian law, traffic data is not considered to be protected by the right to confidentiality of communications, it has to be noted that this may not be the case in other jurisdictions. [↑](#footnote-ref-45)
46. *Eisele,* in: *Schönke/Schröder*, StGB, 28. Aufl., München, 2010, § 238, comment no. 4. [↑](#footnote-ref-46)
47. *Unger*, Spam-Abwehr, DuD 2004, pp. 343; affirmative: *Tschope*, in: *Heidrich/Forgó/Feldmann* (Eds.), Heise Online Recht, 3. EL Oktober 2011, vol. 2, C. chapter III 4.4, comment no. 105. [↑](#footnote-ref-47)
48. *Lenckner/Eisele,* in: *Sch/Sch* (*supra nota* 77), § 206, comment no. 6; *Fischer*, in: *Fischer*, StGB, 57. Aufl., München, 2010, § 206, comment no. 1; *Walter/Kargl*, in: *Kindhäuser/Neumann/Paefgen* (Eds.), StGB, 3. Aufl., 2010, Vol. 2, § 206, comment no. 13. [↑](#footnote-ref-48)
49. *Fischer*, in *Fischer* (*supra nota* 79), § 206, comment no. 7; in regard to the question which facts are covered by the telecommunications secret see: *Lenckner/Eisele* in *Sch/Sch* (*supra nota* 77), § 206, comment no. 6. [↑](#footnote-ref-49)
50. *Ellinghaus*, in: *Arndt/Fezer/Scherer* (Eds.), TKG, Berlin, 2008, § 88, comment no. 13-17; *Fischer*, in *Fischer* (*supra nota* 79), § 206, comment no. 7. [↑](#footnote-ref-50)
51. *Eisele* in: *Sch/Sch* (*supra nota* 77), § 206, comment no. 6; *Fischer*, in *Fischer* (*supra nota* 79), § 206, comment no. 7. [↑](#footnote-ref-51)
52. Regional Court Hamburg, Decision of 23 June 2005, *LG Hamburg*, AZ 631 Qs 43/05, in: *Computerrecht* 2005, p. 832 seq, at p. 833; *Ellinghaus*, in: *Arndt/Fezer/Scherer* (supra nota 81), § 88, comment no. 15. [↑](#footnote-ref-52)
53. German Codes quoted hereafter are official translations available on the website of the German Ministry of Justice (http://www.gesetze-im-internet.de/Teilliste\_translations.html). Whenever such an official translation is not available, translation was provided by the authors of this report and is explicitly stated as such. [↑](#footnote-ref-53)
54. Referring to the different kind of offenders: *Walter/Kargl*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 206, comment no. 19; *Fischer, in Fischer* (*supra nota* 79), § 206, comment no. 2. [↑](#footnote-ref-54)
55. *Walter/Kargl, in: Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 206, comments no. 21-23; *Fischer, in Fischer* (*supra nota* 79), § 206, comments no. 6-9. [↑](#footnote-ref-55)
56. *Schuster,* IT-gestützte interne Ermittlungen in Unternehmen – Strafbarkeitsrisiken nach §§ 202a, 206 StGB, in: ZIS 2/2010, p. 68-75, at p. 73. [↑](#footnote-ref-56)
57. *Lenckner/Eisele* in *Sch/Sch* (*supra nota* 77), § 206, comments no. 10 and 36; Fischer, in Fischer (*supra nota* 79), § 206, comment no. 8. [↑](#footnote-ref-57)
58. *Lenckner/Eisele i*n: *Sch/Sch* (*supra nota* 77), § 206, comment no. 8.; *Braun, Telekommunikation am*

    *Arbeitsplatz, in: Heckmann* (Ed.), Internetrecht. JURIS Praxis Kommentar, 2. Aufl., Saarbrücken, 2009, p. 800, comments no. 97 and 103. [↑](#footnote-ref-58)
59. Translation by Dr. Katharina Ziolkowski. [↑](#footnote-ref-59)
60. See *VGH Kassel*, judgment of 19. May 2009, file no. 6 A 2672/08. Available at http://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=VGH%20Hessen&Datum=19.05.2009&Akte

    nzeichen=6%20A%202672/08. See also: *BVerfGE* 115, p. 166, 184; *Ellinghaus*, in: *Arnt/Fezer/Scherer* (fn 83), § 88, comment no. 20. [↑](#footnote-ref-60)
61. See: *Lenckner/Eisele* in: *Sch/Sch* (*supra nota* 77), § 206, comment no. 13; *Fischer*, in *Fischer* (*supra*

    *nota* 79), § 206, comment no. 9; . *Walter/Kargl*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79),

    § 206, comment no. 44. [↑](#footnote-ref-61)
62. *BGH,* Urt. v. 13.01.2011, III ZR 146/10, comment no. 8. [↑](#footnote-ref-62)
63. *BGH,* Urt. v. 13.01.2011, III ZR 146/10 comments no. 3, 6. [↑](#footnote-ref-63)
64. *BGH,* Urt. v. 13.01.2011, III ZR 146/10, comment no. 8. [↑](#footnote-ref-64)
65. The German Federal Supreme Court explicitly names a period of some days, in which the provider must be given the possibility to react on incoming information about faults and malfunctions (*BGH,* Urt. v.13.01.2011, III ZR 146/10, comment no. 8.). Therefore the period of time is strictly limited to a small number of days, maybe weeks. [↑](#footnote-ref-65)
66. *Fischer*, in: *Fischer* (*supra nota* 79), § 202b, comment no. 10; *Walter/Kargl*, in:*Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 202b, comment no. 11. [↑](#footnote-ref-66)
67. *Eisele* in *Sch/Sch* (*supra nota* 77), § 202b, comment no. 1; *Fischer*, in: *Fischer* (*supra nota* 79), § 202b, comment no. 2. [↑](#footnote-ref-67)
68. *Eisele* in *Sch/Sch* (*supra nota* 77), § 202b, comment no. 3; *Fischer*, in: *Fischer* (*supra nota* 79), § 202b, comment no. 3. [↑](#footnote-ref-68)
69. *Eisele* in: *Sch/Sch* (*supra nota* 77), § 202b, comment no. 3; *Fischer*, in: *Fischer* (*supra nota* 79), § 202b, comment no. 4. [↑](#footnote-ref-69)
70. *Eisele* in: *Sch/Sch* (*supra nota* 77), § 202b, comment no. 4.; *Fischer*, in: *Fischer* (*supra nota* 79), § 202b, comment no. 3. [↑](#footnote-ref-70)
71. See: *Eisele*, in: *Sch/Sch* (*supra nota* 77), § 238, comment no. 13; interestingly, the Federal Police is not responsible for the prosecution of crimes in regard to telecommunication, which often will cross the border of different federal states, see art. 12 of the Federal Police Code. Available at http://www.gesetze-iminternet.

    de/bgsg\_1994/\_\_12.html. [↑](#footnote-ref-71)
72. The details of the responsibilities of a telecommunication service provider are subject to debates within the scholarly writings and jurisdiction, see: *Heckmann*, chapter 1.7 - § 7 Telemediengesetz, in: *Heckmann (*Ed.*)* (*supra nota* 89), comments no. 132 seq. [↑](#footnote-ref-72)