The 1st Korea-Russia Forum on Cybersecurity Law and Policy:

"Reality Check of Cybersecurity Law and Policy"

Date: Monday, 17 December 2018, 12:50~18:00

Venue: Conference Room (Maple Hall, 4th floor) at the Plaza Hotel (Choong-gu, Seoul)

Organizers: Korean Institute of Criminology

International Cyber Law Studies, Korea

Korea University Cyber Law Centre

Far Eastern Federal University Law School

12:50~13:20	Registration	
13:20~13:30	Welcoming Session	Welcoming Remark: In Sup HAN, President (Korean Institute of Criminology)
		Welcoming Remark: Nohyoung PARK, President (International Cyber Law Studies, Korea)
		Welcoming Remark: Roman DREMLIUGA, Vice Dean (Far Eastern Federal University Law School)
13:30-13:40	Group Photo	
13:40~15:00	Session 1: National Developments of Cybersecurity Law and Policy	
	Moderator	- Roman DREMLIUGA, Vice Dean (Far Eastern Federal University Law School)
	Speakers	- Alexander KOROBEEV, Professor (Far Eastern Federal University) - Yaroslava KUCHINA, Professor (Far Eastern Federal University) - Han Kyun KIM, Research Fellow (Korean Institute of Criminology)
	Discussants	- Duk-Jin LEE, Prosecutor (Supreme Prosecutors' Office, ROK) - Jea Hyen SOUNG, Research Fellow (Korean Institute of Criminology)
15:00~15:20	Tea Break	
15:20~16:20	Session 2: Artificial Intelligence in the context of Cybersecurity	
	Moderator	- Joonkoo YOO, Professor (Korea National Diplomatic Academy)
	Speakers	- Roman DREMLIUGA, Vice Dean (Far Eastern Federal University Law School) - Vadim RESHETNIKOV, Student (Far Eastern Federal University Law School)
	Discussants	- Jee-Young Yun, Research Fellow (Korean Institute of

		Criminology)
16:20~17:40	Session 3: International Developments of Cybersecurity Law and Policy	
	Moderator	- Joonkoo YOO, Professor (Korea National Diplomatic Academy)
	Speakers	- Roman DREMLIUGA, Professor (Far Eastern Federal University Law School) - Nohyoung PARK, Professor (Korea University Law School)
	Discussants	- Yaroslava KUCHINA, Professor (Far Eastern Federal University) - Ki Won JUNG (Ministry of Foreign Affairs, ROK) - Myung-hyun CHUNG, Research Professor (Legal Research Institute, Korea University)
17:40~18:00	Final Discussion	

환 영 사

역사적으로 지리적으로 한국과 가까운 러시아는 풍부한 자원과 큰 성장 잠재력을 바탕으로 유라시아 경제연합(EAEU) 출범 등 아태지역 경제 통합 및 개방 움직임을 가속화하고 있습니다. 이에 현 정부도 극동개발을 위한 남·북·러 3각 협력 및 러시아와 협력이 매우 중요하다는 점을 인식하고, 2017년 100대 국정과제에 신북방정책 추진과 한국-러시아 경제협력 강화를 포함시킨 바 있습니다.
뿐만 아니라 대통령직속 북방경제협력위원회를 설립하고, 2017년 9월 한·러 정상회담 및 제3차 동방경제포럼에서 新북방정책 비전 선언 및 한국-러시아간 9개 협력분야인 “9-BRIDGE 전략”구상을 제시하였습니다. 특히 한국과 러시아의 제조업 및 첨단산업 육성 등 산업선진화 정책추진에 공동협력하기 위해 대학, 연구소 및 공공기관 등 연구기반을 활용한 기술협력을 적극 추진하고 있습니다.

한국형사정책연구원 또한 2004년부터 유엔 마약및범죄국(UN Office on Drugs and Crime)과 함께 사이버범죄 및 사이버보안 분야에서의 국제적·지역적 협력과 연구기반을 구축해 왔을 뿐만 아니라, 유엔 범죄방지 및 형사사법연구기관 네트워크 (UN Crime Prevention and Criminal Justice Programme Network) 회원기관으로서 전 세계 50여개 연구기관 및 형사사법기관과 정책연구교류협력 관계망을 맺고 있습니다.

발표와 토론을 위해 러시아에서 방문해 주신 극동연방대학교 법학대학원 (Far Eastern Federal University Law School) R. Dremliuga, Y. Kuchina, V. Reshetnikov, A.Korobeev 교수님께 환영과 감사의 인사를 드립니다. 아울러 한·러 사이버보안 법정책포럼을 함께 준비해 주신 국제사이버법연구회 박노형 교수님과 참석해 주신 여러분들께도 감사드립니다.

모쪼록 오늘 첫 모임을 계기로 한·러 사이버보안 법정책 포럼이 사이버법과 사이버범죄 전문가들의 교류 마당으로 자리 잡아 한국과 러시아 양국의 공동협력 기반을 더욱 튼튼히 해 나갈 수 있기를 바랍니다. 감사합니다.

2018년 12월 17일
한국형사정책연구원
원장 한 인 섭

Welcoming Remarks of Prof. Nohyoung Park (Korea Univ. Law School)

I am glad to say welcoming remarks on behalf of International Cyber Law Studies, Korea, one of the organizers of the first Korea-Russia Forum on Cybersecurity Law and Policy. When I met Prof. Dremliuga at the Far Eastern Federal University Law School last October in Vladivostok, we agreed to cooperate academically for cybersecurity issues between Russia and Korea. Thus, both sides meet today at the Roundtable, which is the first part of this agreed cooperation.

As we all know, cybersecurity is one of the most important and hottest current issues internationally as well as domestically. Cybersecurity is to be assured for the peace and security of our society. Cybersecurity is also very difficult to understand as the nature of cyberspace is quite different from the conventional domains. It also involves rapidly developing technology and slowly following related legal systems.

Now both Korean and Russian experts get together to discuss the legal and policy aspects of cybersecurity in both domestic and international contexts. The Roundtable is a track 2 format in that it is basically between non-governmental experts. However, as the result of the Roundtable could contribute to the governmental policy-making in both countries, the Roundtable may work and develop on track 1.5. I hope that this Roundtable will invite more experts and more institutes in Russia and Korea for wider and deeper discussion soon.

Finally, I am very grateful to the Korean Institute of Criminology, which is a co-host of this Roundtable. And I am very grateful to the participants of this Roundtable from Russia and Korea. I sincerely hope that this Roundtable today should be productive and informative again with all the participants in this room. Thank you

Dremliuga Roman

Vice Dean

Far Eastern Federal University School of Law

Welcome to all participants of the meeting.

It is a big honor to me and my institution to be co-host of the 1st Korea-Russia Forum on Cybersecurity Law and Policy: «Reality Check of Cybersecurity Law and Policy».

I express my gratitude to the President of Korean Institute of Criminology In Sup HAN, as well as to President of International Cyber Law Studies Nohyoung PARK.

This event is devoted to the issue of high importance because cyberspace long time was almost without legal control and transparent rules. The last couple of years Russia tries to propose a new convention that would be helpful in terms of the increase of security level of cyberspace.

I’m pretty sure that such events would be useful for both sides because our institutions could provide a higher level of expertise to policymakers.

Peaceful existence depends largely on the mutual understanding of the parties. I sincerely hope that this meeting will make not only researchers but also our countries more understandable to each other.

[Session 1]

National Developments of Cybersecurity Law and Policy

А.И. Коробеев[1]
Дальневосточный федеральный университет, г. Владивосток, Россия
E-mail: akorobeev@rambler.ru

NATIONAL ASPECTS OF CYBERCRIME IN THE RUSSIAN FEDERATION:

II. The crimes in the area of unmanned aerial systems and national criminal law.

В современной России активно ведутся работы по созданию и внедрению в практику беспилотных транспортных средств (БТС), которые используются в космосе (околопланетные орбиты, межпланетное пространство, атмосфера и поверхность планет), воздухе (земная атмосфера), на суше (городская дорожная сеть, рельсовые линии и др.), водной среде (водная поверхность и подводное пространство), подземной среде (подземные каналы и коммуникации, в том числе трубопроводы и скважины, а также неразработанная порода). Указанные средства производятся как в военных целях, так и для использования в народном хозяйстве, например в логистике, лесоохране и др.

Так, по сообщениям прессы, в России начались работы по проектированию высотного беспилотного аппарата, работающего на солнечной энергии. Новый аппарат сможет применяться на высотах до 30 км, что исключает столкновение с гражданскими авиалайнерами [2]. Создан действующий прототип летающего такси-беспилотника, аналогичного тому, разработки которого ведутся и в других странах (Великобритании, Новой Зеландии, Японии). В русле тех же тенденций развивается и морской (речной) транспорт. Судостроение настроено на развитие безэкипажного

[1] Александр Коробеев, доктор юридических наук, профессор, заведующий кафедрой уголовного права и криминологии Юридической школы Дальневосточного федерального университета. Заслуженный деятель науки РФ.

[2] См.: *Вальченко С.* В России построят «солнечный» беспилотник-гигант // Московский комсомолец. 2018. 7 июня.

судоходства. Планируется в будущем строить подобные суда разных типов: научно-исследовательские, спасательные, транспортные и др.[3] С 2015 г. в России активно развиваются технологии, необходимые для создания беспилотных автомобилей. 22 июня 2018 г. беспилотный автомобиль «Яндекса» совершил первую большую поездку из Москвы в Казань. Преодолев 780 км, машина в пути находилась 11 час (в дневное и ночное время), при этом 99 % времени двигалась в автоматическом режиме, соблюдая все скоростные ограничения. В 2018 г. в «Сколково» запустили опытную зону для поездок на беспилотном общественном транспорте. Условия управления им приближены к тем, что есть на дорогах общего использования.

При этом в мировой практике дорожного движения уже зафиксированы дорожно-транспортные происшествия с участием беспилотников.

Первая авария произошла во Флориде (США) в мае 2015 г., в результате столкновения с другим автомобилем погиб оператор, находившийся в кабине беспилотника. В Tesla считают, что причина случившегося может состоять в том, что автоматика, под управлением которой находилось транспортное средство, не успела распознать опасность из-за белого цвета прицепа грузовика на фоне яркого неба. По другой версии, автопилот мог дать сбой из-за длинного свеса прицепа фуры и большого дорожного просвета, что помешало автоматике «увидеть» препятствие[4].

Вторая трагедия произошла 21 марта 2018 г., когда спортивный внедорожник Uber насмерть сбил переходившую дорогу женщину. При этом в кабине «автономно-управляемой машины» сидел оператор, предусмотренный как раз на случай экстренных ситуаций. «…Было бы очень сложно избежать этого столкновения в любом режиме – автономном или с водителем – основываясь на том, как она (велосипедистка) выскочила из тени прямо на дорогу… Uber вряд ли виноват в этом инциденте, – заявила шеф

[3] См.: Комсомольская правда. 2018. 6 апр.
[4] *Ломакин Д.* Первая жертва автопилота // Газета.ru.

полиции г. Темпе С. Моир. – Ни камеры, ни человек, сидевший в кабине испытываемого автомобиля, не заметили велосипед до момента столкновения. В частности, водитель понял, что произошло столкновение, только услышав его звук. Автомобиль, оснащенный двумя камерами, также не предпринял попытки затормозить. Машина двигалась со скоростью 38 миль в час (61 км/час) в зоне с ограничением скорости в 35 миль в час»[5].

В обоих случаях не было выявлено каких-либо дефектов в технике, которые могли бы спровоцировать аварийную ситуацию[6]. Но не был решён и вопрос об уголовной ответственности за причинённый вредтиз-за пробелов в уголовном законе США.

Россия также практически не развивается в разработке законодательства в сфере использования роботомобилей. 30 марта 2016 г. состоялся круглый стол на тему «Нормативно-правовое регулирование применения беспилотных систем в Российской Федерации», организованный Комитетом по науке и наукоемким технологиям. По результатам обсуждения были подготовлены рекомендации Государственной Думе, в частности предлагалось внести изменения в Правила дорожного движения, ГК РФ[7] и УК РФ[8].

На наш взгляд, помимо указанных отраслей права требует изменений и дополнений КоАП РФ, а также целый ряд федеральных законов: ФЗ «О безопасности дорожного движения», ФЗ «Об автомобильных дорогах и дорожной деятельности в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» и др. Между тем в недавно принятой «Стратегии безопасности дорожного движения в Российской Федерации на 2018 – 2024 годы» о беспилотных транспортных средствах нет даже упоминания[9].

---

[5] РИА Новости // https:/ria.ru/world/20180320/1516807246.html

[6] *Забродина Е.* Нечеловеческий фактор // Российская газета. 2018. 21 марта.

[7] Предлагалось изменить редакцию ст. 1079 ГК РФ таким образом, чтобы понятия «автомобиль» и «транспортное средство» охватывали и понятие «беспилотное транспортное средство».

[8] Duma.gov.ru/news/12015/.

[9] См.: Российская газета. 2018. 25 янв.

Очевидно, что на нынешнем этапе создания нормативно-правовой базы, регламентирующей порядок функционирования БТС, а также основания и условия ответственности за нарушение этого порядка (т.е. в ситуации практически полного отсутствия такой базы), можно говорить лишь о разработке некоего алгоритма, позволяющего сконструировать цепь последовательных действий, направленных на построение в конечном итоге замкнутого контура искомой нормативно-правовой системы.

Такого рода действиями должны быть признаны, например, разработка стандартов, технических регламентов и правил функционирования (управления движением и эксплуатацией) беспилотных транспортных средств с учетом известной специфики, которой обладают современные традиционные виды транспорта. Разработку указанных нормативов придется осуществлять применительно к конкретным видам БТС.

Правовую неопределенность в этой сфере необходимо будет преодолевать как на уровне международного права, так в национальных законодательствах.

В сентябре 2018 г. эксперты из многих стран рассмотрели проект поправок к Венской конвенции о дорожном движение 1968 г., которые приравнивают действия автоматизированной системы управления автомобилем к вождению машины человеком. Проект поправок инициирован и подготовлен российскими экспертами Национальной технологической инициативы (НТИ) «Автонет». Документ будет рассмотрен на Всемирном форуме по безопасности дорожного движения Комитета по внутреннему транспорту Европейской экономической комиссии ООН (ЕЭК ООН). Вконвенцию, в частности, предлагается ввести определения терминов «высокоавтоматизированное транспортное средство» и «среда штатной эксплуатации» - это эксплуатационные, географические, временные, дорожные, инфраструктурные и иные условия, для функционирования в которых специально предназначена автоматизированная система вождения. Таким образом, беспилотники получат право передвигаться не по всем

дорогам общего пользования, а лишь по оборудованным специальными датчиками и метками, по которым машины будут ориентироваться.

В дальнейшем аналогичные изменения должны быть имплементированы в национальные законодательства, в том числе и в российское[10].

Подобные правовые процедуры необходимо будет осуществить и применительно к другим видам БТС.

Однако, с наибольшим количеством проблем столкнется отечественный законодатель в процессе регламентации именно уголовной ответственности за преступления данной категории. Остается открытым вопрос о персональной ответственности физического лица – субъекта транспортного преступления; самую острую проблему здесь составят поиск и определение именно субъекта преступления – лица, совершившего преступление.

Поскольку состав нового вида транспортных преступлений будет сконструирован, скорее всего, по типу материального, у правоприменителя в процессе его квалификации возникнут сложности с определением конкретного пункта нарушенных виновным правил безопасного управления БТС и не меньшие – с установлением причинной связи между нарушенными правилами и наступившим преступным результатом. Предполагаем, что значительное количество такого рода транспортных преступлений будет совершаться в ситуации так называемого «неосторожного сопричинения», а это еще больше осложнит поиск и установление лица, совершившего преступление.

Несмотря на отмеченные сложности, возьмём на себя смелость утверждать: допустимость, возможность и целесообразность установления в обозримом будущем нового уголовно-правового запрета в сфере обеспечения безопасности транспортной деятельности вполне очевидны.

[10] См.: Шадрина Т. Беспилотникам оформляют права // Российская газета. 2018 8 авг.

Что же касается технико-юридического его оформления, то тут возможны варианты. Оптимальной, с нашей точки зрения, выглядит следующая парадигма.

А. Нам представляется, что уголовно-правовой запрет должен быть сформулирован в виде единой, универсальной нормы, распространяющей свое действие на все виды беспилотных транспортных средств.

Конструирование норм об ответственности за транспортные преступления должно базироваться на принципах единообразного и унифицированного формулирования диспозиций и санкций этих норм. Указанные элементы должны быть согласованы между собой в рамках не только отдельных статей, но и всей системы в целом. Такая согласованность достижима лишь при условии отказа от использования в качестве ведущего критерия различных видов транспортных средств.

Изложенное предопределяет необходимость наброска (хотя бы в самых общих чертах) определенных требований, которым должен отвечать уголовно-правовой запрет абсолютно нового вида (типа) девиантного поведения в сфере транспортной деятельности.

Прежде всего отметим тот, очевидный для нас факт, что возможная в ближайшее время криминализация нового вида транспортных преступлений будет полностью отвечать требованиям, предъявляемым доктриной уголовно-правовой политики к основаниям установления уголовно-правового запрета. Известно, что криминализация транспортного преступления может быть признана научно-обоснованной лишь при учете законодателем совокупности целого ряда факторов, важнейшими из которых являются: определенная степень общественной опасности деяния, его относительная распространенность и типичность, неблагоприятная динамика данного вида транспортного правонарушения, возможность воздействия на него уголовно-правовыми средствами, невозможность успешной борьбы менее репрессивными мерами, отсутствие негативных побочных последствий

запрета, наличие материальных ресурсов для его реализации, определенный уровень общественного правосознания и психологии населения[11].

Вряд ли можно будет найти веские аргументы, объясняющие необходимость объединения в одной норме ответственности за нарушение правил безопасности движения и эксплуатации железнодорожного, воздушного, морского, внутреннего водного транспорта, метрополитена и невозможность включения в нее ответственности за аналогичные нарушения на других видах механического транспорта. Связь между железнодорожным и морским транспортом уловить столь же непросто, как и между воздушным и автомобильным. Если законодатель и сейчас не усматривает различий в специфике преступлений на таких видах транспорта, как железнодорожный, водный и воздушный, установив ответственность за их совершение в одной норме, то нет оснований полагать, что особенности посягательств на безопасность функционирования других видов механического транспорта столь существенны, что не позволяют сформулировать все эти преступления в виде единого состава[12].

Б. Поскольку диспозиция искомой статьи с неизбежностью будет носить бланкетный (отсылающий к иным законам) характер, предлагается состав преступления сконструировать по типу материального, взяв за основу те признаки объективной стороны (речь идет о последствиях), которые фигурируют в чч. 1, 2 и 3 ст. 263 УК РФ. При этом никаких дополнительных частей (вроде тех, что можно обнаружить сегодня в ст. 264 УК РФ) конструировать не придется.

В. Субъект преступления должен быть только специальный. Однако трактовка его, на наш взгляд, должна быть достаточно широкой. Данный элемент состава преступления должен включать в себя: а) персонифицированных разработчиков конкретной компьютерной программы, предназначенной для конкретного БСТ; б) лиц, контролирующих безопасную

[11] См.: Коробеев А.И. Транспортные преступления и транспортная преступность. М., 2015. С. 419.
[12] Подробнее об этом см.: Коробеев А.И. Указ. соч. С. 427-428.

эксплуатацию этих программ; в) владельцев БСТ, обязанных осуществлять текущий контроль за безопасными условиями их эксплуатации; г) лиц, находящихся в БСТ и осуществляющих непосредственный контроль за безопасностью его эксплуатации.

В примечании к статье УК РФ, устанавливающей уголовную ответственность за нарушение правил безопасности функционирования (движения или эксплуатацию) беспилотных транспортных средств, целесообразно дать законодательное определение понятия БСТ.

Такой (в самых общих чертах) нам видится «дорожная карта» разработки российской нормативно-правовой базы, призванной урегулировать весь комплекс вопросов, связанных с появлением и внедрением в практическую человеческую деятельность еще одного достижения четвертой промышленной революции – беспилотных транспортных средств.

Yaroslava Kuchina
Associate Professor
Far Eastern Federal University

NATIONAL ASPECTS OF CYBERCRIME IN THE RUSSIAN FEDERATION:
I. The main issues of anti-cybercrime policy and legal regulation of the Russian Federation.

1. Traditionally, there is an opinion that the Russian Federation is among the top 3 countries that are the attack source states of the global threat to cyber security, along with the United States and China. However, if we turn to official sources and expert opinions, like NTT 2018 Global Threat Intelligence Report, we will see that the tendency to reduce the impact of "Russian hackers" in high-profile cyber-attacks has been decreased for more than two years, and in 2018 Russia did not even enter the top five global "threats" of cyber security.

2. A similar gap also exists in the statistics data on cybercrime in Russia. Unofficial numbers, like those from experts and analysts of the banking sector, and the largest developers of antivirus programs and others show the enormous figures of damage caused by domestic cybercriminals, while the statistics of official bodies, for example, the Prosecutor General's Office of the Russian Federation, are much less. What caused this difference? First of all, the fact that the first group traditionally mixes various categories of offenses, and not all of them are crimes prohibited by the Criminal Code of the Russian Federation. At the same time, the representatives of the prosecutor's office and the Investigative Committee of the Russian Federation have repeatedly spoken about the difficulties of initiating criminal cases about cybercrimes committed in the banking sector, because of the unwillingness of banks to admit the fact of crime openly because of the possible losses in reputation.

3. The second reason is more narrow - it is that the Criminal Code of the Russian Federation itself. The Criminal Code is the only source of criminal prohibition in Russia and its cybercrime system is very different from that in Russian science, and, moreover, in the field of cybercrime expertise, where experts are not usually lawyers. Let's highlight it in more details

4. Analysis of the Criminal Code of the Russian Federation allows to distinguish three groups of crimes, two of which contain a reference related to digital area, cyber rights, etc., and one has nothing to do with them. Thus, the public relations associated with the use of digital technologies, were identified in law long before the emergence of the term "digital economy" and interest in cyber security - in Chapter 28 of the Criminal Code of the Russian Federation. It establishes liability for crimes in the field of computer information. The sections and chapters of the Special Part of the Criminal Code contain in their headlines a list of standardized public relations protected by criminal law – so called objects of crime. The field of computing information is one of them.

Chapter 28 of the Criminal Code of the Russian Federation currently contains four elements of a crime:
1) Art. 272 "Illegal access to computing information";
2) Art. 273 "Creation, use and distribution of malicious computing software (programs)";
3) Art. 274 "Violation of the rules of operation of the means of storage, processing or transmission of computing information and information-telecommunication networks";

4) Art. 274.1 “Illegal impact on the critical information infrastructure of the Russian Federation”.

Two other crimes are contained in Chapter 21 of the Criminal Code of the Russian Federation “Crimes against another's property”:
1) Art. 159.3 "Fraud in the field of electronic banking systems"
2) Art. 159.6 “Fraud

These two groups of crimes use the term “computing information” in their definitions and refer law enforcers to the entire cyber rights sector of the Russian Federation. Some slides later, we take a closer look how this happens.

The third group of crimes is general structures that criminalize common crimes, which contain in the wording a special qualified clause that can be translated as **“if the crime was committed using the Internet”.** This clause refers to the so-called qualifying clauses and provides for more serious punishment, which is caused by the special method of a crime’s committing, like here - the capabilities of the Internet. For example, art. 110.1 **“Declination to suicide”** provides for the induction via the Internet as such a qualifying aggravating symptom. It allows the criminal responsibility for such “modern” cybercrime as cyberstalking and cyberbullying, which are not in the Russian Criminal Code in the definitions.

5. However, this leads to the fact that only crimes of Chapter 28, two types of fraud and a few of more than 30 crimes from the third group are included in the official statistics as cybercrimes. Moreover, the statistics of the Supreme Court do not include these few crimes from group 3 in the cybercrime group. The final result of this distinction is so: criminal law of Russia has only "computing crimes", and cybercrime is the term of academics and cybersecurity organizations.

6. So that is why all the rest of our presentation here is a closer look at “computing crimes”, in particular – the “computing information” crimes in the criminal law of Russia.

7. The main is Art. 272 of the Criminal Code, which provides criminal liability for illegal access to legally protected computer information, if this resulted in the destruction, blocking, modification or copying of computer information (part 1). In the article notes, computer information is defined as ***information (messages, data) presented in the form of electrical signals, regardless of the means of storing, processing and transmitting them***. That is, the object of the crime under Art. 272 - public relations that ensure the legitimate access, creation, storage, modification, use of computer information by its creator, as well as the use of this information by other users.

8. Until March 7, 2011, the wording of art. 272 was different. The previous edition relied on the State Standards of 1987 and 1990s. According to them, the object of the crime was an electronic computing machine, ***the main functional devices of which are made on electronic components***; including PC (personal computer), the computer system, and so on/ In other words - ***a set of programs designed to ensure a certain level of efficiency of the information processing system due to the automated management of its operation and a specific set of services provided to the user.***

Turning to the concept of “computer information”, the legislator expanded the possibility of interpreting the legal meaning of the object and the subject of the crime, eliminating technical details and focusing on the signs of the protected phenomenon. The computer information is

the information, messages or data expressed in a certain form - in the form of electrical signals. The purpose and characteristics of such information do not matter.

9. There is no separate explanation for the concept of “computer information” definition in the law of Russia. The papers refer to the Recommendations of the General Prosecutor's Office on investigating computing crimes, but these Recommendations are not the rule of law.

10. The objective side of the crime under Part 1 of Art. 272 of the Criminal Code of the Russian Federation, formed by three elements: the criminal action, socially harmful consequences and a direct causal link, that is, according to the legal doctrine, the material crime (crime with consequences). **The legislator defined the act as illegal access to legally protected computer information.** This, in turn, determines the methods of committing a crime, although they are not listed in the disposition of the any cybercrime article. An exhaustive list of consequences includes such a result of criminal actions as the destruction, blocking, modification or copying of computer information – all illegal.

11. At the same time, the wording “legally protected computer information” makes the object of a crime under Part 1 of Art. 272 of the Criminal Code so called blanket or linked. In its meaning, it refers to Art. 2 of Federal Law 27.07.2006 No. 149-Ф3 “On Information, Information Technologies and Information Protection”. In the clause 1 of this law ***information*** is defined as “***information (messages, data) regardless of the form of their presentation”.*** That information is protected by the law and has at least three forms - information, messages and data. The note 1 to Art. 272 of the Criminal Code adds to this form another characteristic – it should be ***a form of electrical signals***, thereby delimiting computer information from other information.

12. The rule about “information protected by law” is applied to information as a whole, not only computing one. This issue is resolved quite simply - the types of information protected by law are determined by the list of specified laws. For example, art. 13 of the Federal Law of 21.11.2011 No. 323 establishes that information about the fact of a somebody’s seeking medical help, the state of personal health and diagnosis, other information obtained during the medical examination and treatment constitute a ***medical secret***, disclosure of which in any form is not allowed and protected by laws, including criminal law. That is ***protected information access to which is restricted – means protected.***

In Part 2 of Art. 9 of the Federal Law of July 27, 2006 No. 149 there is a list of information, access to which is restricted. Such a restriction is established by federal laws in order to protect the fundamentals of the constitutional system, morality, health, rights and legitimate interests of other persons, ensure the defense capability and security of the state, and the types of information protected by law include information constituting a commercial secret, official secret and other secrets; information about an individual, including information constituting a personal or family secret, personal information (personal data).

Other laws distinguish additional types of such protected information: professional secrecy (law, medical), or objects of copyright and related rights, which are often, in their external form, means **data**. That is an exhaustive list of protected information, that also separates it from unprotected information. Information may become protected no only by a rule of law, but also by a court decision, which has the power specifies it from the total amount of all such information in a particular. For example, issues affecting the rights and legitimate interests of minors are not considered in open court.

The law also recognizes as protected the information that can be identified by any of the ways, access to which is determined by its legal operator. For such protection it is only needed the prohibition of the operator to get such access, established by any acts or contract. Violation of this prohibition, entailing the consequences prohibited by the Criminal Code, constitutes a crime.

13. The result of such regulation is so: ***if all the protected information from above has acquired the form of digital data of any kind, even the type of Word or PPT document (doc, ppt, pdf, jpg format or so), it becomes protected by the Criminal Code – art. 272 and other "computing crimes" articles.*** It means – such information should not be *personal* in the meaning, for example, of the GDPR or Safe Harbor Principles.

14. The objective side of the described crimes is fully determined by the special form of the subject of the crime. The act, according to the Code, must constitute illegal access, which entailed certain consequences: the destruction, blocking, modification or copying of computer information. By them is meant the following:

- destruction of information - bringing information or its part into an unusable state, regardless of the possibility of its recovery;
- information blocking - the impossibility for some time or constantly to perform the required operations on information completely or in the required mode, that is, performing actions that restrict or block access to computer equipment and resources located on it, targeted obstruction of access of legitimate users to computer information not related to its destruction;
- information modification - illegal introduction of changes in computer information (the criteria of illegality is determined in accordance with article 1280 of the Civil Code of the Russian Federation according to the formula "by contradiction");
- copying information — creating a copy of existing information on another medium, that is, transferring information to a separate carrier while maintaining the original information unchanged, or reproducing information in any material form — by hand, photographing text from the display screen, and reading information by intercepting any information and etc.

15. If unauthorized access, that is, the action itself and the method of its commission, are derived from the type of computer information, then the socially dangerous consequences of this action are the same. As we noted above, the list of consequences is exhaustive. The application of the criminal law rules is not made dependent on the device for processing and transmitting computer information. Computer-protected information is the same information that is protected by law in other forms - visual, verbal, written, etc. In practice, it is often assumed that this is information downloaded on a PC, laptop or other relative device, on the Internet, etc., (information in the form of electrical signals), and called digital or cyber information, or just **data**. However, this rise to some practical challenges, which are not obvious from the texts of the Code's articles.

16. Digital data (or we called it in this presentation by the term "computing information") differs from other types of information by several essential features, the main of which is the conscious nature of its location. Information becomes digital due to the commission of a number of technical actions. That means, in legal terms, it cannot acquire the "form of electrical signals" on its own, or as a result of unconscious human activity, such as audio

information (for example, free speech). The legislator introduced into the article 272 a sign of the independence of computer information from the means of its storage, processing and transmission, but did not consider that the field of information technology imply almost total legal certainty which is established by law or by contract. The consequence of these for the Russian digital world is so: almost 100% of the informational components if they turn digital are protected in the meaning of the Criminal Code. Unfortunately, this is impossible to implement practically.

In the case of a crime under Art. 272 of the Criminal Code, and other computing crime articles, the question of the presence or absence of a crime should be decided by conducting a legal examination and establishing limits of "protection by law" with respect to each type of digital information. Moreover, because of the complexity and multi-layered architecture of the modern digital technologies the limits of protection can (and should) be identified more than once in relation to the same crime object, if the consequences of the criminal act harm different types of the information (f.e. – hacking the iPhone and deleting the info in it from the different storages).

17. This means that the result of a crime must be covered by the intent of the subject of the crime. There will be no criminal legal consequences of an action that is carried out regardless of the will of the person or his knowledge that the action will happen. And the method of committing a crime, the criminal consequences should correspond to the type of computer information, its technical characteristics and features.

18. As a result, the determination of the presence or absence of *corpus delicti* in the actions of a person is entirely dependent on the legal regimes applied on the digital signals the Russian legislator considered as "computing information". This means that the more detailed the legal regulation of data, information and the virtual world in general, the more required the involvement of different experts (technical and legal) to establish all elements of such cybercrime in the forms in which they now exist in the Criminal Code. The only way to resolve the current situation may be the transition from such criminal prohibitions to more general ones. The possible way of it will be clear from the second part of the presentation.

Current Law and Policy on Cybersecurity of Korea

The 1st Korea-Russia Forum on Cybersecurity Law and Policy:
"Reality Check of Cybersecurity Law and Policy"

Han-Kyun Kim
Research Fellow
Korean Institute of Criminology

hankyun@kic.re.kr

1.1. What is 'Cybersecurity'

- " securing the legitimate function of cyberspace and the safety of information by combat against cyber-attacks for the purpose of protecting national security and national interest."

National Cybersecurity Act of Korea (Government Bill of 2017) Art.2.④

1.2. What it the matter with ‘Cybersecurity’

- South Korea is a prime target for cyber-attacks due to the country’s high network connectedness, advanced use of mobile devices, and significant intellectual property.

- According to Akamai (www.akamai.com/Cyber-Security), a U.S.-based cloud service provider, around 97 percent of South Korea’s population had internet access in 2017. South Korea has the fastest average internet speed in the world, at 28.9 megabytes per second (Mbps).

1.3. What it the matter with ‘Cybersecurity’

- South Korea leads the world in mobile broadband penetration, with over 120 percent of all South Korea’s population (as of the 3rd quarter of 2017).

- The government projects the internet speed will be 10 times faster by 2020, which could transform Korea’s technological capabilities and make it an “ultra-connected nation.”

1.4. Cybersecurity as national security

- South Korea recognizes that cyber-security is a matter of national security. Although the country boasts one of the world's fastest and most mobile IT infrastructures, it also has an insecure infrastructure which is vulnerable to cyber-attacks. The country has heightened its security protocols over recent years.
- Hackers have previously targeted government agencies in South Korea, which compromised sensitive information and endangered the welfare of government officials and civilian employees alike.
- The frequency and gravity of cyber-attacks has prompted the South Korean government to re-evaluate its cyber-security strategy.

1.5. Cyber threats from North Korea

- The first key challenge in relation to South Korean cybersecurity is that South Korea faces an ever-present cyber threat from North Korea. After the end of the Cold War, North Korea lost its allies–the Soviet Union and China–and began to focus on the development of unconventional security strategies, such as cyber capabilities, to compete with South Korea.
- North Korea currently operates about 6,000 cyber warfare troops and conducts cyber warfare, including the interruption of military operations and attacks against major national infrastructure, to cause psychological and physical paralysis in the South.

1.6. Cyber attacks from North Korea

- The worst problem is that the South Korean government cannot officially attribute these several critical cyber attacks to North Korea.
- The first reason is related to the characteristics of cyber attacks: they are easy to deny and extremely difficult to attribute to the attackers. After being attacked, a state cannot easily find decisive evidence or accurate proof, so the state has to rely heavily on circumstantial evidence for attribution.

1.7. Cyber attacks from North Korea

- The second reason is the Chinese government has been uncooperative in providing information about the cyber attacks. Due to a lack of critical information infrastructure necessary to execute cyber attacks within North Korea, North Korean hackers are frequently stationed in China.
- Because China has not cooperated with South Korea's investigations, the South Korean government has failed to trace and identify North Korean hacking organizations. Thus, South Korea needs to build new partnerships with other countries, especially China, to solve these challenges.

1.8. Institutions for Cybersecurity

- National Cyber-Security Center (National Intelligence Service)
- Korea Internet & Security Agency (KISA)
- National Police Agency's Cyber Terror Response Center
- These agencies are responsible for identifying, preventing, and responding to cyber-attacks and security threats.
- Authorities have investigatory powers of law enforcement: National Intelligence Service; National Police Agency Cyber Bureau; Forensic Science Investigation Department of the Supreme Prosecutors' Office; Financial Supervisory Service; and KISA.

1.9. Institutions for Cybersecurity

- Ministry of Science and ICT
  http://english.msip.go.kr/index.do
- Korea Communications Commission
  http://eng.kcc.go.kr/user/ehpMain.do
- Korea Internet & Security Agency (KISA)
  http://www.kisa.or.kr/eng/main.jsp
- Korea Information Security Industry Association (KISIA)
  http://www.kisia.or.kr/new_kisia/english/e_s1_menu1.html
- Korea Institute for ICT Promotion
  http://www.kiat.or.kr/site/main/index/index002.jsp

2.1. Patterns of Cybersecurity legislation

- data protection and the protection of privacy,
- criminal law to address cybercrimes,
- protection of intellectual property,
- protection against illegal and harmful content,
- criminal procedural law,
- legal regulations on security measures such as cryptography and digital signatures

2.2. Current laws in Korea

- Personal Information Protection Act
- Act On The Protection Of Information And Communications Infrastructure
- Act on Promotion of Information and Communications Network Utilization and Information Protection
- Electronic Financial Transactions
- Credit Information Use and Protection
- Act on the Protection, Use, etc. of Location Information
- Act On Prevention Of Divulgence And Protection Of Industrial Technology
- Special Act On The Prevention Of Loss Caused By Telecommunications-Based Financial Fraud And Refund For Loss

2.3. Cybercrime-related laws in Korea

- Criminal Act of 1953, as amended in 1995
- Act on Promotion of Information and Communications Network Utilization and Information Protection (amended in 2018)
- Act on the Protection of Information and Communications Infrastructure (amended in 2018)
- Act on the Protection of Communications Secrets (amended in 2018)
- Act on the Protection of personal information (amended in 2017)
- Act on the Protection of credit information (amended in 2018)
- Copyright Act (amended in 2018)
- Act on Digital Signatures (2017)

3.1. Patterns of Cybercrimes in Korea

- The Classification of Cybercrime in National Police Agency Cyber Bureau
- Crimes of Information Network System Infringement
- Crimes Involving the Use of Information Network Systems
- Crimes involving Illegal Contents

3.2. Cybercrime statistics

	Total (총계)		Crimes with Information Network Infringement (정보통신망침해범죄)		Crimes involving the use of Information Network (정보통신망이용범죄)		Crimes involving Illegal Contents (불법컨텐츠범죄)	
	Occurred (발생)	Arrested (검거)	Occurred (발생)	Arrested (검거)	Occurred (발생)	Arrested (검거)	Occurred (발생)	Arrested (검거)
2014	110,109	71,950	2,291 (H:1,648;D:26; M:130;O:487)	846 (H:540;D:16; M:69;O:221)	89,519 (I:56,667;E:15,596; P:939;C:14,168; O:2,149)	56,461 (I:40,657;E:6,567; P:635;C:7,198; O:1,404)	18,299 (P:4,354;G:4,271; D:8,880;S:363; O:431)	14,643 (P:3,739;G:4,047; D:6,241;S:300; O:316)
2015	144,679	104,888	3,154 (H:2,247;D:40; M:166;O:701)	842 (H:524;D:19; M:74;O:225)	118,362 (I:81,849;E:14,686; P:609;C:18,770; O:2,448)	86,658 (I:68,444;E:7,886; P:296;C:8,832; O:1,200)	23,163 (P:4,244;G:3,352; D:15,043;S:134; O:390)	17,388 (P:3,475;G:3,365; D:10,202;S:124; O:222)
2016	153,075	127,758	2,770 (H:1,847;D:192; M:137;O:594)	1,047 (H:537;D:164; M:98;O:248)	121,867 (I:100,369;E:6,721; P:2,410;C:9,796; O:2,571)	103,172 (I:89,364;E:4,034; P:2,125;C:5,616; O:2,033)	28,438 (P:3,777;G:9,538; D:14,908;S:56; O:159)	23,539 (P:3,435;G:9,394; D:10,539;S:53; O:118)
2017	131,734	107,489	3,156 (H:2,430;D:43; M:167;O:516)	1,398 (H:990;D:28; M:122;O:258)	107,271 (I:92,636;E:6,066; P:413;C:6,667; O:1,489)	88,779 (I:80,740;E:2,632; P:298;C:4,134; O:975)	21,307 (P:2,646;G:5,130; D:13,348;S:59; O:124)	17,312 (P:2,329;G:5,080; D:9,756;S:52; O:95)

<출처:경찰청 사이버 안전국>

3.3. Crimes of Information Network System Infringement

- Cases of intrusion into computers or information network systems (computer systems) without justifiable access privileges or access which exceeds permitted access privileges or causing damage, destruction, or alterations to systems, data, programs and causing disruptions (impairing performance or causing system failures) in communications networks

- Hacking, Denial-of-Service Attack, Malicious programs, Other Information Network System Infringement Crimes

3.4. Crimes Involving the Use of Information Network Systems

- Cases where information network systems (computer systems) are the main means to commit the acts which correspond to the fundamental elements of the crime

- Internet Fraud, Electronic Communication Financial Fraud, Personal/Location Information Infringement, Cyber Copyright Infringement Spam Mail, Other Types of Crime Using Information Network Systems

3.5. Crimes involving Illegal Contents

- The distribution, sale, lease, or display of goods, services, or information which is prohibited by law through information network systems (computer systems

- Cyber Pornography, Cyber Gambling, Cyber Defamation/Insult, Cyber Stalking, Other Illegal Contents Crime

4.1.Hacking(unauthorised access)

- Under the Act on Promotion of Information and Communications Network Utilization and Information Protection(the Network Act), it is prohibited for anyone to infiltrate another's information communication network (ICN) without authorised access or beyond the scope of authorised access. Any violation shall be subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million.
- Under the Electronic Financial Transactions Act(the EFTA), any unauthorised access of electronic financial systems shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

4.2. Denial-of-service attacks

- Under the Network Act, it is prohibited to cause disruption of an ICN by intentionally disturbing network operations with large volumes of signal/data or superfluous requests. Any violation shall be subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million.
- Also, under the EFTA, any attacks on electronic financial systems using programs such as a computer virus, logic bomb or email bomb with the intention of destroying data on, or disrupting the operation of, electronic financial systems shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

4.3.Phishing

- For the regulation of phishing crimes, the Special Act On The Prevention Of Loss Caused By Telecommunications-Based Financial Fraud And Refund For Loss (Special Act on Financial Fraud) has been enacted.
- Under the Special Act on Financial Fraud, anyone found guilty of phishing crimes shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

4.4.Infection of IT systems with malware

- Under the Network Act, it is prohibited for anyone to transmit or distribute malware that can damage, destroy, alter, falsify or disrupt the operation of ICN systems, data or programs, without a justifiable cause.
- Any violation shall be subject to imprisonment of not more than seven years or a penalty of not more than KRW 70 million.

4.5. Possession or use of hardware, software or other tools used to commit cybercrime

- The use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools) is prohibited under the Network Act.
- Any violation shall be subject to imprisonment of not more than seven years or a penalty of not more than KRW 70 million.

4.6. Identity theft or identity fraud

- Under the Personal Information Protection Act (PIPA), anyone who commits, or aids and abets, the illegitimate acquisition of personal information, being processed by another party for subsequent provision to a third party for commercial gain or for illegitimate purposes, shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.
- Under the Network Act, it is prohibited for anyone to collect another person's information, or induce the provision of another person's information, through the ICN by deceptive means. Any violation shall be subject to imprisonment of not more than three years or a penalty of not more than KRW 30 million.

4.7.Electronic theft

- Any theft of the company's critical information by a company's employee or former employee shall be punished under the Criminal Act as a breach of fiduciary duty or under the Act on Prevention of Unfair Competition and Protection of Trade Secrets as divulging of trade secrets.
- Any such theft shall be subject to imprisonment of not more than 10 years or a penalty of not less than KRW 30 million under the Criminal Act and imprisonment of not more than five years or a penalty of not more than KRW 50 million under the Act on Prevention of Unfair Competition and Protection of Trade Secrets.
- Any infringement of the employer's copyright shall be subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million.

4.8.Failure by an organisation to implement cybersecurity measures

- Under PIPA and its Enforcement Decree, personal information processors have the obligation to implement technical, managerial and physical measures in order to procure security, such as establishing internal control plans and storing access records to ensure personal information is not lost, stolen, leaked, falsified, altered or damaged.
- In the event personal information is lost, stolen, leaked, falsified, altered or damaged due to a person's failure to implement such measures, such person shall be subject to imprisonment of not more than two years or a penalty of not more than KRW 20 million.

5.1. Protective measures for network security

- Under the PICIA, managerial organisations have the obligation to establish and implement managerial measures, including physical and technical measures (such as prevention, backup, recovery, etc.), to safely protect the critical ICN infrastructure facilities and managerial data.
- Under the Network Act, any ICN service provider must take protective measures to procure the security of ICN used in the provision of ICN services and the reliability of information.

5.2. Protective measures for network security

- Organisations that operate and manage collective ICN facilities ("Collective ICN Facility Operator") for the ICN service of third parties must take the following protection measures for the secure operation of ICN facilities:
- (i) technical and managerial measures for access control and monitoring of unauthorised access to ICN facilities;
- (ii) physical and technical measures for the protection of ICN facilities from natural disasters and threats, such as terrorist attacks, and for procuring the continuous and secure operation of ICN facilities;
- (iii) hiring and assignment of personnel for the secure management of ICN facilities;
- (iv) establishment and implementation of internal control measures (including emergency plans) for the secure management of ICN facilities; and
- (v) establishment and implementation of technical and managerial measures to prevent the dissemination of infiltration Incidents.

5.3. Protective measures for network security

- Under the Network Act, the ICN provider or a Collective ICN Facility Operator must report any "infiltration Incidents" (defined as Incidents due to attacks on the ICN or the related information system through hacking, a computer virus, logic bomb, email bomb, denial of service, high-powered electromagnetic wave, etc.) to the Ministry of Science and ICT or KISA immediately upon the occurrence of such infiltration Incident.
- Under PIPA, in the event of any leakage of personal information which concerns 10,000 or more persons, the personal information processor must report such leakage and subsequent measures, without delay, to the Ministry of Interior and Safety or KISA.

5.4. Protective measures for network security

- Under PIPA, once a personal information processer becomes aware of any leakage of personal information, it must notify the owner of the leaked personal information, without delay, of the following:
- (i) the type of personal information that has been leaked;
- (ii) the timing and circumstances of the leakage;
- (iii) the actions that the owner of the personal information can take to minimise any damages resulting from the leakage;
- (iv) the protective response measures taken by the personal information processor and relief procedures; and
- (v) the name and contact of the department to which the owner of the leaked personal information (who has incurred damages) can file a report.
- Under the Credit Information Act, in the event of any credit information leakage, the above items must be notified to the owner of such credit information.

5.5. Protective measures for network security

- With regards to the financial services sector, the Credit Information Act and the EFTA prescribe specific legal requirements for financial institutions.
- With regards to the telecommunications sector, the following companies need to obtain a certification as to whether they satisfy the prescribed technical and physical protective measures for the security and reliability of ICNs:
- (i) companies such as telecommunication providers or companies who provide information through the telecommunication provider's ICN, whose annual revenue or income is not less than KRW 150 billion; or
- (ii) companies such as telecommunication providers or companies who provide information through the telecommunication provider's ICN, whose revenue for the preceding fiscal year is not less than KRW 10 billion or whose average volume of daily users for a three-month period is not less than 1 million.

6. Key elements necessary to secure cybersecurity in Korea

- Establishing national strategy on cybersecurity;
- Ensuring that the breaches of security and cybercrimes have been defined in the law;
- Establishing legal investigative powers to combat cybercrime;
- Developing mechanism to promote regional and international cooperation in cybersecurity;
- Pursuing these in a manner that provides safeguards that protect fundamental human rights and freedoms.

National Cybersecurity Act (Government Bill of 2017)

- Aims of the Act
- Cybersttacks bring vast amount of damages to national economy and cause social turmoil, and thus threatens national security
- There needs special policies to prevent and minimize the risk and damage of cyberattacks
- Legal basis for establsing and systematizing national institutions for cybersecurity

National Cybersecurity Act (Government Bill of 2017)

- Presidential Commission of National Cybersecurity
- Mandates : making national policy and strategy for cybersecurity
- Members : Chief Secretary for National Security, Deputy ministers of government ministries, national assembly, national courts, constitutional court
- Accountable institutions and support institutions
- critical institutions which taking accountability of protecting cyberspace, designated by the NIS

National Cybersecurity Act (Government Bill of 2017)

- National Plans on Cybersecurity
- The Director of NIS establishes the National Basic Plan every 3 years
- Government ministries and local governments establish annual action plan of the Basic Plan
- Review of Cybersecurity
- The Director of NIS shall have the powers to review cybersecurity-related works of government ministries

National Cybersecurity Act (Government Bill of 2017)

- Sharing information of cyber threats
- The NIS established its own Center for Sharing Information of Cyber threats
- Accountable institutions are obliged to provide ther own information on cyber threats
- The director of the Center shall provides measures to protect personal rights against any threats

National Cybersecurity Act (Government Bill of 2017)

- Detecting cyberattacks
- Head of the accountable institution shall establish its own security control center to detect and anlayse cyberattacks
- Notice of the incidents and investigation
- Head of the accountable institution shall make notice of any incidents to its higher institutions,
- Head of the higher institutions shall take investigation on the cause and damage of the incidents to prevent further damage
- Any incidents threatening national security shall be investigated by the NIS

National Cybersecurity Act (Government Bill of 2017)

- Alert against cyber-cisis
- The Director of the NIS issues alerts against cyber-crisis
- Higher accountable institutions can establish headqueters for cyber-crisis control as to the critical alerts

※ NIS Cyberthreats Warning system

- If the NIS detects any sign of a cyber threat against government or public institutions, IT networks and ascertains concrete threats, it issues a warning, indicating the level of risk.

[Session 2]

Artificial Intelligence in the context of Cybersecurity

Roman Dremliuga, Vadim Reshetnikov
Far Eastern Federal University

Legal issues of using AI to predict and prevent crimes

With the development of technologies of Artificial Intelligence (AI), the policing authorities from all over the world are tempted by the possibility to use such technologies in order to predict and prevent crimes. Intellectual systems open new horizons for struggle against crime, both organized and opportunistic, that could not have been imagined before. The concept that was shown almost 15 years ago in a science-fiction movie «Minority Report» has now become a reality. The police can know exactly when, where, and even by whom a crime is going to be committed, and all of this is because of the abilities of special predictive AIs. But what are these predictive AIs exactly? What are they capable of? And is it legal to use such technologies? The present essay tries to answer these questions.

A market overview: what are the nature and capabilities of existing predictive AIs?

The AI technologies are being used more and more widely by governmental structures all across the globe these days. The policing agencies are among these structures. The police try to use the boundless potential of the AI in their fight against the crime. The policing agencies of such countries as the United States, China, Japan, Israel and Chile can be acknowledged as the pioneers of this field. The products they use are already not just working prototypes, but fully-operative crime-predicting systems.

The first notable product in sphere of crime predicting AIs is PredPol software, developed by scientists from University of California in collaboration with Los Angeles Police Department. Predpol is being used across the US[1], and, in test regime, in Uruguay's capital Montevideo[2], British county of Kent[3] and Japanese prefecture of Kanagawa[4]. Predpol uses only three variables: type, time and scene of unfavorable event[5]. The data of criminal's identity is not included into information being processed by the software, making the system very unpersonalized. By using crime

---

[1] *See* RESOLUTION NO.: R-2013-025 Authorizing the City Manager to execute a Software Subscription Agreement between the City of Columbia and PredPol, Inc. (City Council of the city Columbia); *available at:* https://www.columbiasc.net/depts/city-council/docs/old_downloads/02_19_2013_Agenda_Items/Resolution_2013_025_Software_Subscription_Agreement_PredPol_Inc.pdf
As well as Regular Meeting ALHAMBRA CITY COUNCIL July 28, 2014; *available at:* http://www.cityofalhambra.org/imagesfile/agenda/201506/minutes_2014_07_28_113658.pdf
And PredPol website; *available at:* http://www.predpol.com/news;

[2] *See* Kyra Gurney, *Using Data to Predict and Prevent Crime in LatAm* (Feb. 23, 2015); *available at:* https://www.insightcrime.org/news/analysis/using-data-to-predict-and-prevent-crime-in-latam;

[3] *See* http://www.predpol.com/tag/kent-police;

[4] *See* Joshua Nevett, *The Real Minority Report: Police trial AI to predict and prevent crimes before they happen* (Jan. 29, 2018); *available at:* https://www.dailystar.co.uk/news/world-news/677796/artificial-intelligence-japan-kanagawa-police-predict-minority-report-2020-olympics;

[5] *See* The PredPol Algorithm *available at:* http://www.predpol.com/technology;

reports from wide periods of time (years and even decades), the algorithm defines the districts, where is the highest probability rate of potential crimes.

Hitachi, famous electronics manufacturer, offers its own module of criminal activity prediction as a part of a global smart-city complex «Hitachi Visualization Suite» (HVS). The module is named Predictive Crime Analytics (PCA) and, instead of operating predetermined data, uses machine learning technologies[6]. System's developers claim that PCA can define unobvious behavior patterns better than any other similar product in the market. PCA considers datas of criminal activity, road traffic, public transportation routes, video from surveillance cameras, weather and even messages in social networks.

Similar algorithm is used by a system, developed by CEAMOS, Chilean Center for Analysis and Modeling of Security. But, in addition to analyzing data, this system has an ability to create different simulations of forthcoming events and make predictions based on the outcomes of such simulations[7].

Another developer in this sphere is Tel-Aviv-based company Cortica. Cortica offers a product of city-wide cameras systems, that, in a non-stop regime, transfer video data to a server, where data is being processed and analyzed by a neural network. This neural network is capable of identifying high-risk situations on the streets and potential crimes[8]. In addition to smart-cameras, Cortica provides fully-automated smart-drones, which increase surveillance coverage drastically[9].

In China, in the same time, the government uses, along with analyzing systems, similars to the ones described above, innovative technologies of face recognition. The software presented by a startup CloudWalk is capable of identifying a person in a video tape through face recognition, moreover this software works in a real-time basis and can analyze simultaneously up to several thousands people on a tape[10].

Another Chinese startup, UniWiew, tracks individuals who frequently travel to sensitive countries like Myanmar and Vietnam and automatically marks them as suspicious[11].

How legal is to use predictive AIs?

The majority of existing systems, which aim is to predict crimes, that are yet to be committed, or, at least, identify areas or events with high risk of criminal activity, make their predictions based on a merit of analysis of big data. In this regard, the concerns are growing of how legal is to use such systems. The scholars see here two

---

[6] Hu Yoshida, *Predictive Crime Analytics provide Safer Policing and Safer Police* (May 25, 2016) *available at:* https://app-hds.jiveon.com/community/innovation-center/hus-place/blog/2016/05/25/predictive-crime-analytics-provide-safer-policing-and-safer-police;

[7] *See* Angel Luis Vazquez, *La inteligencia artificial aplicada a la prevención de delitos* (Sept. 24, 2017), *available at*: https://yip-online.es/la-inteligencia-artificial-aplicada-a-la-prevencion-de-delitos;

[8] Milenka Peña, *¡Como en Minority Report! Un sistema de inteligencia artificial predice crímenes* (Apr. 15, 2018); *available at:* https://es.digitaltrends.com/computadoras/prediccion-crimenes-cortica-inteligencia-artificial;

[9] *See* Cortica website; *available at:* https://cortica.com/smartcity/index.html;

[10] *See* Yi Shu Ng, *China is using AI to predict who will commit crime next* (Jul. 24, 2017), *available at:* https://mashable.com/2017/07/24/china-ai-crime-minority-report/#aJmWRct7PqqR;

[11] *Id.*;

fundamental issues: collection of a big data without a person's permission; and usage of predictions based on this data for further legal prosecution.

It is widely assumed that collecting big data should be considered as acceptable and even appropriate. Such view was presented by, among others, American authors in context of how big data technologies *distort traditional Fourth Amendment rules that protect citizens against unreasonable searches and seizures by law enforcement*[12]. Thus, Andrew Guthrie Ferguson draws an analogy between big data and traditional small data collected by the policemen themselves[13]. In this context, all the data legally collected by the public services through videotapes from surveillance cameras (visual big data) or from analysis of police records (defying behavior patterns), has the ground for creating «a reasonable suspicion[14]». In the majority of most authoritative jurisdictions video surveillance (CCTV) is considered legal, especially with respect to protection against theft, violence, terrorism or other similar issues that can be regarded as severe threats to society[15]. And, though video surveillance is a subject to different limitations[16], that vary depending on existing legislations of different countries[17], it is globally accepted as a tool of preserving public safety, and, thus, can be processed by an authorized agency, in particular through the usage of predictive AIs.

The more controversial question is legality of collecting and using personal information from the Internet. In the past, before the first general rules of data protection were formed, it was thought that any data available in a public access can be processed without limitations. It was changed, however, with the adoption of new generation of legal data regulations[18]. Generally, personal data can still be processed by the operator, and even transferred to a third party (an operator of a predictive AI system in the case of this topic), but the following of special procedures is now obligatory[19]. Thus, in a formal sense, predictive AIs can legally process big data, but, in order to comply with existing international rules, the states are obliged to

---

[12] Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev. 327 (2015);

[13] *Id. 327, 376*;

[14] Reasonable suspicion has been defined as «specific and articulable facts that taken with rational inferences of those facts warrant belief that criminal activity afoot» - *See* United States v. Sokolow, 490 U.S. 1, 7 (1989); Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race and the Future of Law Enforcement*; N. Yo. U.P., 63 (2017);

[15] Mahmood Rajpoot, Q., & Jensen, C. D. (2015). *Video Surveillance: Privacy Issues and Legal Compliance*. In V. Kumar, & J. Svensson (Eds.), *Promoting Social Change and Democracy through Information Technology* IGI global, 6-7;

[16] For example limits of the storage time of recorded images, the need for notification signs in the surveillance area and the possible requirement of a court warrant in order to perform surveillance on a particular person;

[17] *See e.g.* Video Camera Surveillance (Temporary Measures) Act 2011 - New Zealand; The Surveillance Camera Code of Practice 2013 (the 'SCCOP') - UK; Act on the Protection of Personal Information (Act No.57 of May 30, 2003) - Japan;

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

[19] GDPR, Article 6, 1(c),(d),(e),(f); Article 9;

implement special procedures of legitimizing such actions into their internal legislation.

«A Minority Report problem» - a prediction of a crime does not take into account a possibility of a criminal abandoning the perpetration

The second vital issue of legality of usage of such systems is understanding whether or not the prognosis made by the AI is sufficient enough for legal prosecution. Although, according to American researchers and policing authorities, these predictions have a ground basis to create «a reasonable suspicion» that a suspect is involved in crime (which is, within the established by the U.S. Constitution procedures, sufficient to proceed to arrest of a suspect[20]) it is vitally needed to keep in mind that any prognosis given by a predictive AI, regardless to how fair it is, shows only one possible outcome.

It is a distinguishing feature of a human being to have a freewill. Precisely a freewill gives a human being who intends to commit a crime a possibility to stop at any moment, even when all the preparations for an act of crime have been finished. And here comes a fundamental question, which deals with both law and ethics: «Are interests of public safety and security above the right of a person to have an opportunity for a voluntary refusal[21]?»

A voluntary refusal is not a universally acknowledged right, though. Its application and even existence varies in different legal systems. Although quite usual in continental law[22], the institution of voluntary refusal is missing in common law system[23]. That leads to the situation when every state has to develop legal regulations of usage predictive AIs depending on existence of such right. Thus, in those states where voluntary refusal is not an integral part of their national criminal legislations, the procedures of legal prosecution based on AI's data can be established. Otherwise, other measures can be created of how to use this data.

Prevention but not enforcement

The so-called «Heat List» developed by Illinois Institute of Technology can be regarded as example of such measures, different from criminal prosecution. «The Heat List» algorithm analyzes big data, and, by using 11 variables, creates risk scores for every citizen of Chicago[24]. The algorithm shows the risk of being victim or perpetrator of gun violence. The statistics is horrifying: up to 70% of all people shot in Chicago in the last years were correctly identified on the list[25]. In Chicago such list itself cannot be regarded as ground basis for prosecution. However, Chicago Police

---

[20] Terry v. Ohio, 392 U.S. 1, 21-22 (1968);

[21] Voluntary refusal is a principle of a criminal law that gives criminal a right not to be prosecuted if he voluntarily and definitively abandons a perpetration of an unlawful act.

[22] *See* The U.S. Model Penal Code, Section 5.01 (4); Texas Penal Code, Section 15.04; Russian Criminal Code, Article 31;

[23] Ray Moses, *Inchoate Crimes & Complicity* (2004); *available at:* http://www.crimesanddefenses.com/SilverBulletsIII.html;

[24] Nissa Rhee, *Can Police Big Data Stop Chicago's Spice in Crime?,* Christian Sci. Monitor (June 2, 2016); Monica Davey, *Chicago Police Try to Predict Who May Shoot or Be Shot,* N.Y. Times (May 23, 2016);

[25] Andrew V. Papachristos, *Commentary: CPD's Crucial Choice: Treat Its List as Offenders or as Potential Victims?,* Chi. Trib. (July 29, 2016);

try to intervene in the lives of those in the list in other ways. The policemen pay the visits to people identified by the algorithm as targeted and give these people «The Custom Notification Letters» that inform individuals of the arrest, prosecution, and sentencing consequences of continuing being engaged in public violence[26].

Great possibilities do mean great responsibility

Such types of preemptive measures themselves cannot provide a guarantee of a perpetration being prevented, however the statistics shows a decrease of a criminal activity. But more importantly, unlike legal prosecution, such preemptive therapy does not create an opportunity for the governmental authorities, tempted by the possibilities, to use predictive AIs and algorithms for establishing a totalitarian control over the population.

Intelligent systems, that are capable to predict the possible outcomes of events by analyzing big data, can be used for different purposes other than crime prediction. A complex analysis of habits, tastes and typical behavior, based on video surveillance or activity in social networks can be of service for both commercial and non-commercial causes. And if targeted advertising, that is located in a grey zone of ethics and law, does not really harm someone's life, politically-driven usage of big data, on the contrary, potentially does. For example, totalitarian governments can easily identify political views of their citizens and, thus, suppress those who oppose them. AIs might serve such governments by predicting any protests and helping them to crush an opposition once and for all. Such measures are already being widely used by Chinese authorities in Tibet and Uyghur regions[27].

The AI's ability of analyzing and evaluating situation, together with ubiquitous video surveillance, can become crucial in defeating crime, but, at the same time, create an opportunity for establishing a regime of unseen before totalitarianism. Thus, a question rises: «Is it worth to continue working on developments in this sphere, even regarding the possible outcomes?»

[26] Chi. Police Dep't, *Custom Notifications in Chicago, Special Order S10-05 IV.D* (Oct 6, 2015), *available at* https://directives.chicagopolice.org;

[27] *See An internment camp for 10 million Uyghurs; Meduza visits China's dystopian police state* (Oct.1, 2018), *available at* https://meduza.io/en/feature/2018/10/01/an-internment-camp-for-10-million-uyghurs;

[Session 3]

International Developments of Cybersecurity Law and Policy

Dremliuga Roman

Roman Dremliuga, PhD in Law

Vice Dean School of Law

Associate Professor

Far Eastern Federal University

Vladivostok, Russia

Russian view on international cooperation in sphere of combating cybercrime

History of development

Over recent decades the Computer technologies have dramatically transformed social landscape by connecting individuals, institutions, businesses, and agencies all over the world. Despite the fact that the net has improved the information management, developed social network, created new areas of entertainment and provided solutions for global challenges, it also has introduced new risks, threats and dangers for societies and states.

The key technology that influenced on societies, states and cultures became the Internet. It came to Russia in 1994 that was much later than in North American and European countries. After the Soviet period, during democratization in the 90-s, the freedom of speech was widely recognized as critical to liberal modernization in Russia. Basis of democratic strategy was the development of open communication networks. The internet became a perfect opportunity to create independent information space. The government and the society didn't predict negative consequences and gave the Internet a lot of credits. At the time when domain ".ru" was only registered in InterNIC (The Internet's Network Information Center), there were a lot of legal acts against cybercrimes in Europe and North America but not in Russia.. At first the Russian-language internet provided weak opportunities for cyber offenders, but starting from the ground up, Russia has quickly built a vast information infrastructure.

The indicator that Russia became state with cybercrime threat is adoption of new Criminal Code. It was adopted by Russian Federation in 1996 with The Chapter 28 "Crimes in the Sphere of Computer Information" that contained first provisions criminalized cybercrimes[1]. The provisions of the chapter have been amended a lot of times and supplemented by new cyber articles in the other parts of the Criminal Code.

That time a computer crime was not regarded as a crime by Russian people and the government. In accordance with liberal reforms principals and establishing of liberal society the most

[1] 'Ugolovnyy kodeks rossiyskoy federatsii' [The Criminal Code of the Russian Federation] Number 63-FZ of June 13, 1996. The Code was published Sobranie Zakonodatelstva Rossiiskoi Federatsii [The Collection of Legislative Acts of the Russian Federation] of June 17, 1996. Item. 25, p. 2954.

common supported idea was the idea of full freedom of information limited only by the industrial standards and sometimes criminal law[2]. Even information threatened the integrity of the State or promoted racism was common for the Russian internet that time. There was no social concern on cyber terrorism or hacking. Hackers generally were recognized as genius people who sometimes accidentally or because of curiosity infringed the law[3] and usually people didn't associate them with other traditional types of crimes.

Acts enacted by the Russian Government and the President reflected problem of the cybercrime ignoring. For instance, the Federal Program of the Russian Federation for Enhancing Fight against Crime for the Years 1994 – 1995 adopted by decree of the President had no mentions or provisions on computer crimes, cybercrimes or crimes in the sphere of computer information. The Federal Program was devoted to fight against organized crime and terrorism, counteract to crimes against person and property, struggle against economic crimes and corruption; international cooperation in the crime combating, etc. The Federal Target Program for the Enhancement of Fighting Crime in the Years 1996 – 1997 adopted by the government of the Russian Federation didn't pay attention to the problem of cybercrime either.

Recognition of threat and Convention on Cybercrime

In the 2000-s the cybercrime became a major threat inside and outside the Russian Federation, and the trend of internationality of cybercrimes requested new attitudes to the issue. This was clearly reflected in the steps taken by the Russian Federation. First of all, Russia concluded Agreement on the cooperation of participants of the commonwealth of independent states in the fight against with crimes in the sphere of computer information in 2001.

This agreement consists of 17 articles. It defines four types of crimes that the states parties in accordance with the Agreement undertake to adopt in their criminal legislation. These types are: 1) unlawful access to computer-protected information by law; 2) the creation, use or distribution of malicious programs; 3) violation of the rules of operation of a computer, computer system or their network; 4) illegal use of computer programs and databases that are objects of copyright.

The most detailed part of the Agreement is a description of the procedure for sending and executing a request for assistance (Art. 6-8). The Agreement also enshrines the rules relating to the use of confidential information received from the competent authority of another State (Article 9).

When Russia tried to create regional instruments to fight against cybercrime it was obvious that cybercrime became a global problem. In March 2001, the United Nations Commission on Crime

[2] Bachilo I.L., 'Potentsial zakonodatel'stva v protsessakh stanovleniya informatsionnogo obshchestva' [The Potential of Legislation in the Processes of the Information Society Formation] (1999), Information Society, Issue 3. Russia, Moscow. 40-45.

[3] Dremliuga, Internet-crimes, 2008.

Prevention and Criminal Justice submitted a special report prepared in response to Resolution 1999/23 of July 28, 1999. The cybercrime experts presented their classification of information technology crime in the above report.

It is worth noting that it was this classification that formed the basis of the first international legal act criminalizing various forms and types of cybercrime. On November 23, 2001, the Convention on Cybercrime was concluded in Budapest.

As underlined in preamble of convention it was created with "recognition of the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies; and with believe that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters"[4].

Convention entered into force in 2004. And the Russian government was going to join the convention. On November 15, 2005, the President of the Russian Federation signed an order "On the signing of the Convention on Cybercrime," in which the head of state gave relevant instructions to the Russian Ministry of Foreign Affairs.

Nevertheless, the Russian Federation has so far not signed this convention. Moreover, on March 22, 2008, the President of the Russian Federation issued Order No. 144-rp " On recognition of the invalidation of the decree of the President of the Russian Federation of November 15, 2005 №. 557-rp "On the signing of the Convention on Cybercrime".

There were a lot of reasons why Russia did not sign the Convention on Cybercrime. One of the main obstacles preventing the Russian Federation from adopting the convention is the fact that the criminal legislation of the Russian Federation does not have a liability of a legal entity in principal. This provision is spelled out in the text of the Convention and is applied in a number of foreign countries.

Article 12 «Corporate liability» underlines that each party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offense established in accordance with this Convention. Of note, Russia still has not recognized the concept of criminal liability of legal persons but only natural persons.

The second obstacle was Article 32 «Trans-border access to stored computer data with consent or where publicly available». Clause "b" of this article underlined that «a party may, without the authorization of another Party … access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary

[4] CONVENTION ON CYBERCRIME, Budapest, 23.XI.2001 http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

consent of the person who has the lawful authority to disclose the data to the Party through that computer system». In accordance with the position of the representatives of the Russian Federation, this provision «may damage the sovereignty and national security of the member states, the rights and legitimate interests of their citizens and legal entities».

Despite Russia doesn't sign the Convention on Cybercrime, it implements some provisions of convention of domestic law. For instance, Russia adopts in Criminal law all provisions of Section 1 «Substantive criminal law» except Article 12 «Corporate liability». Moreover, Russia has similar provisions in sphere of stored computer data and traffic information.

Russia still considered international cooperation as one of the main priorities in the sphere of cyberspace regulation. In "The strategy of the information society development in the Russian Federation" adopted in February 2008 Russia defined one of the direction of development as "Participation in the formation of international information security, improving cooperation between law enforcement authorities of the Russian Federation and foreign states in the area of prevention, detection, suppression and elimination of consequences of the use of information and communication technologies for terrorist or other criminal purposes".

The state program of the Russian Federation "Information Society (2011-2020)" was endorsed by the Order of the Government of the Russian Federation in 2010[5]. Among implied results of the Program was the compliance with requirements of Russian law by telecommunication market participants and control of cybercrime rate on the world average level.

Despite active involvement in the fight against the global problem of cybercrime, Russia has often been criticized by the countries of Europe and North America for not participating in Convention on Cybercrime 2001. Russia had objective reasons to not join the Convention. Its economy mostly depended on resource extraction and weapons production and society and government had no sufficient concern on the issue of cybercrime.

Digital Economy

Priorities were changed when society and government in Russia recognized the necessity of economic transformation. It was obvious that the Russian economy had a low level of digitalization. After long debates and discussions, it was decided that Russia had to modernize its economy and public institutions in terms of digital transformation. One of the first enacted official documents in this sphere was a new Doctrine of Information Security of the Russian Federation that replaced the old Doctrine of 2000.

Among other goals the Doctrine recognizes "promoting the formation of an international information security system aimed as at countering threats to the use of information technologies

[5] The State program of the Russian Federation "Information Society (2011-2020)" endorsed by Order of the Government of the Russian Federation Number (2010). 1815-r of October 20, 2010. The Collection of Legislative Acts of the Russian Federation, Item 6026, (46).

in order to violate strategic stability, as well as at consolidation an mutual strategic partnership in the field of information security, and also to protect the sovereignty of the Russian Federation in the information space". It implied that Russia intended to propose new just international regulation in the sphere of cyberspace regulation.

The next step was the program of Digital Economy of the Russian Federation was approved by the Government of the Russian Federation in its resolution No. 1632-r dated July 28, 2017.

As Russia's Prime Minister Dmitry Medvedev said «The program goal is to organize systemic development and rollout of digital technologies across all spheres of life - in economy, in business as social activity and in public administration, social sphere and municipal economy»[6]. The program consists of five areas dedicated to normative regulation, education, human resources, development of research competencies and IT infrastructure and cybersecurity.

In accordance with the text of the program "The digital economy is represented by the following 3 levels, which in their close interaction affect the lives of citizens and society as a whole:

markets and sectors of the economy (areas of activity), where the interaction of specific subjects (suppliers and consumers of goods, works, and services);

platforms and technologies where competencies are formed for the development of markets and industries (fields of activity);

an environment that creates the conditions for the development of platforms and technologies and effective interaction of market entities and sectors of the economy (spheres of activity) and covers regulations, information infrastructure, personnel, and information security".

The mentioned documents and many others adopted in 2016-2018 show that Russia seriously took up the modernization of the economy. It implies that Russia has to be involved more active into the global fight against cybercrime.

Draft of a new convention

As everybody knows almost every year from 1998, Russia has sponsored a resolution of General Assembly called "Developments in the field of information and telecommunications in the context of international security." It was the platform by which UN member states express their concern about malevolent activity in cyberspace. It was the resolutions that created the Group of Governmental Experts on Cybersecurity in 2004/5, 2009/10, 2012/13, 2014/15, and 2016/17.

The Convention on Cyber Crime had provisions that were potentially dangerous in terms of Russian security and sovereignty but Russia regarded it vitally important to have a document that regulates cyberspace. Due to sanctions and cold confrontation with NATO states Russia also desired to limit external intrusion into internal policy through the Internet. The decision was to propose a new convention that would become a new constitution of cyberspace regulation. As

[6] http://tass.com/economy/958455

fairly commented some Russian officials "The international community needs a unified legal base to combat increasing cyber-crime amid rapid advances in technology"[7].

In 2017 Russia proposed a draft for a new «United Nations Convention on Cooperation in Combating Information Crimes». As a problem of external interference also was an issue for China, it supported the Russian initiative as well as some other states. The draft includes 72 articles, covering supervision of Internet traffic by states, «codes of conduct» for the Internet and «cooperation on investigation» of malicious activity.

In accordance with translation from Russian Embassy «the purposes of this Convention shall be as follows:

a) to promote and strengthen measures aimed at effectively preventing and combating crimes and other unlawful acts in the field of ICT (information and communications technologies);

b) to prevent action directed against the confidentiality, integrity and availability of ICT as well as the misuse of ICT by providing for the punishability of such acts, as described in this Convention, and by providing powers sufficient for effectively combating such crimes and other unlawful acts, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by developing arrangements for international cooperation;

c) to improve the efficiency and develop international cooperation, including in the context of training and providing technical assistance in preventing and combating ICT crimes»[8].

Despite wide endorsement this initiative is not supported by the United States, the European Union, Canada, Japan, Australia and some other countries.

Disagreement policy was clearly expressed in 2018 during the seventy-third session of UN general assembly. Russia and the United States tabled two different the draft resolutions on the same topic. The Russian Federation proposed the draft resolution "Developments in the field of information and telecommunications in the context of international security" (document A/C.1/73/L.27.Rev.1), the First Committee of General Assembly of UN approved it, by a vote of 109 in favor to 45 against, with 16 abstentions. The United States proposed draft resolution «Advancing Responsible State Behaviour in Cyberspace in the Context of International Security» (document A/C.1/73/L.37), with 139 in favor to 11 against, with 18 abstentions. There were a lot of states that voted for both drafts. As said some representatives of such states « the two proposed mechanisms can complement each other, … the two processes to be established by both drafts are not incompatible to each other». That implies that there is no serious disagreement in terms of position but disagreement on the leadership of Russia and China in this sphere.

[7] https://www.rt.com/op-ed/418862-cyber-crime-security-internet/
[8] https://www.rusemb.org.uk/fnapr/6393

Most criticized provision of proposed draft and resolutions is the ban on interference in the internal affairs of other States. As Washington post remarks «The Kremlin's proposed convention would enhance the ability of Russia and other authoritarian nations to control communication within their countries». In the draft of convention it is reflected Article 3 as «the States Parties shall carry out their obligations under this Convention in accordance with the principles of state sovereignty, sovereign equality of States and non-intervention in the domestic affairs of other States» and «this Convention shall not entitle a State Party to exercise in the territory of another State the jurisdiction and functions that are reserved exclusively for the authorities of that other State in accordance with its domestic law»[9]. In resolution it is formulated as "States should not use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability, and reaffirm the right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news, which can be interpreted as interference in the internal affairs of other States or as being harmful to the promotion of peace, cooperation and friendly relations among States and nations"[10].

Both draft and resolution remark the significant role of the UN in training and providing broad assistance in the implementation of rules and initiatives to combat cybercrimes.

Conclusions

Based on the analysis conducted, Russia has a consistent policy regarding the creation and participation in institutions aimed at combating cybercrime. For a long time, this area remained outside the key priorities of the Russian Federation due to the nature of the economy and the internal political situation. In connection with the transition to a digital economy, Russia began to look for an opportunity to secure global and national cyberspace from external interference. The approach proposed by Russia does not contradict the existing order of things but rather complements it. Despite this, Russia's initiative is rejected by the United States and its allies on this issue due to political reasons.

[9] https://www.rusemb.org.uk/fnapr/6393
[10] https://undocs.org/A/C.1/73/L.27

Law Enforcement Access to Data: a Case of the US CLOUD Act (a tentative version)

17 December 2018

Prof. Nohyoung Park
Korea Univ. Law School

CyberLawCentre
innovation | safety | security
KOREA UNIVERSITY

Globalization of Criminal Data

- The *Microsoft Ireland* case in the US courts shows an aspect of the law enforcement's difficulties in coping with globalization of criminal data.
  - Dating back to December 2013, the case involved a dispute between Microsoft and the US government regarding the reach of the Stored Communications Act (SCA).
    - The data, i.e., the contents of all of the emails stored in a particular @msn.com email account, being sought resided on servers in Ireland, which Microsoft personnel could reach from their US keyboards as a matter of fact.
    - The SCA did not contemplate cloud computing when it was enacted into law, and thus much of American law relating to government access to electronic data held by third parties was in fact drafted several years before email was commonly used and the World Wide Web was even created.
  - The US has long argued that its warrant authority requires US-based service providers like Microsoft to turn over responsive data, regardless of where the underlying ones and zeroes happen to be held.
  - Microsoft argued that this authority only extended to data located within the territorial boundaries of the US, and disputed its extraterritoriality.
    - If the data is stored in a foreign country, the US could not compel production via a US-issued warrant.
    - Instead, it would be required to make a mutual legal assistance (MLA) treaty request for the data and rely on the foreign government to access the data and turn it over back to the US.

Globalization of Criminal Data

- The *Microsoft Ireland* case in the US courts shows an aspect of the law enforcement's difficulties in coping with globalization of criminal data.
  - Microsoft lost the case in 2014, but won an appeal in the Second Circuit in 2016.
  - The US Supreme Court heard argument on the case in February 2018.
  - Immediately following the CLOUD Act's passage in late March 2018, the US Department of Justice asked the US Supreme Court to drop the pending *Microsoft* case as moot.
    - The DOJ did alternatively use the CLOUD Act to issue a new warrant for the data held by Microsoft in Dublin.

Globalization of Criminal Data

- Technological developments are driving fundamental changes in the importance of cross-border data requests for law enforcement purposes.
- Law enforcement is facing growing challenges in accessing both data at rest and data in transit.
  - Data at rest includes the emails, social network information, and vast array of other content that increasingly is stored in the cloud.
  - For law enforcement in Europe and most of the world, this evidence is often physically stored in the US or held by a US company that follows the relatively strict probable cause rules of the Electronic Communications Privacy Act (ECPA) of the US.
  - In either instance, the court order or other legal process used in the country where the crime occurred is not sufficient to get this data at rest.
- Police and prosecutors face also similar difficulties in accessing data in transit.
  - With the shift to the secure HTTPS protocol for many communications, encryption means that a wiretap in the country of the crime very often can not provide access to the content.

Globalization of Criminal Data

- Where law enforcement cannot access either data at rest or data in transit in its own country, then it increasingly must seek access to stored records in the cloud.
  - Under the ECPA, for the content of communications, that typically means foreign law enforcement must use the MLA process and show probable cause of a crime to a US magistrate.
  - MLA requests usually were for cross-border crimes, such as drug smuggling or money laundering.
  - Increasingly, MLA requests are for local crimes where emails or social networks contain key evidence but are held abroad.
  - As even these routine local crimes enter the MLA process, law enforcement is seeking streamlined ways to access evidence across borders.

Globalization of Criminal Data

- Again law enforcement faces the globalization of criminal data.
  - In the course of a lawful investigation, they often seek content of communications, increasingly kept in the cloud, often in a different country.
  - In the old days, for a murder or other serious crime in Seoul for example, the police could find the evidence in Seoul.
  - Today web mails, social network posts, and other content are often held across international borders, in the majority of cases in the hands of US-based service providers.
- But the ECPA prohibit US-based companies from turning over communications content to foreign governments, even when those foreign governments are seeking data on their own citizens in connection with a local crime.
  - The only way Korean law enforcement can get this evidence is to make a diplomatic request for the data to the US, employing the time-consuming MLAT process.

Globalization of Criminal Data

- Law enforcement may also have access to unprecedented data on suspects, including location information by tracking cellphones, comprehensive metadata based on all of personal texts, emails, and social network posts, and the numerous other databases of the big data world.
- Both law enforcement and privacy advocates thus point to technological trends that make their respective tasks, i.e., law enforcement and privacy protection, much harder than before.
- Providers of email, social network, and other cloud services also find themselves in the middle between legitimate law enforcement requests and privacy concerns in the government's gaining access to the unprecedented wealth of electronic evidence.

Globalization of Criminal Data

- There has been a recent effort to reform a process for accessing to cross-border data in other way than the MLA process.
- For example, the US and the UK were reported to reach an agreement in 2016 in order for the UK government to be able to make certain categories of requests directly to US-based service providers, without the need and consequent delay of going through the MLA process.
  - The Assistant Attorney General of the US sent a letter to the President of the US Senate, Mr. Biden, requesting a legislative proposal leading to the amendment of the ECPA on July 15, 2016.

Globalization of Criminal Data

- The efforts to reform a process for the access to cross-border data may be complicated by at least three issues.
  - Recent legislative developments in the US and the EU may signal a change in the approach to cross-border data transfer for law enforcement purposes.
- First, large differences still exist in the criminal procedure of different countries.
  - Far more work will be needed to understand how these legal differences can fit within an emerging system for cross-border data sharing.

Globalization of Criminal Data

- Second, a reform is more difficult because there exists a gap of the data protection level among different countries.
  - US privacy advocates understandably express concern at any reduction in the probable cause standard, while EU privacy advocates express concern at transferring data to a jurisdiction that lacks the level of the EU's data protection law.
- Third, the MLA process generally applies to cross-border requests to share information for law enforcement purposes.
  - There is also a need to share information for intelligence and military purposes among different countries.
  - This issue is likely to be more significant in practice, since the relationship between law enforcement and intelligence investigations varies substantially in different countries.

Globalization of Criminal Data

- MLA reform discussions to find a workable legal process will have broader implications in at least two ways.
- First, one reason for supporting MLA streamlining is to reduce the risk of localization of data, which requires emails and other sources of evidence to be stored within the national jurisdiction subject to local procedures.
  - Data localization is in principle against the US approach.
- Second, MLA reform discussion implicates two other hot surveillance issues:
  - As the investigation of even local crimes often involves evidence held abroad, law enforcement will be likely to consider three choices: (1) breaking encryption; (2) hacking into the remote computer before data is encrypted; or (3) using the MLA process to gain the evidence through legal process.

The CLOUD Act of the US

- On March 23, 2018, the US Congress passed, and President Trump signed into law, the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which creates a new framework for government access to data held by technology companies worldwide.
  - Between 2015 and 2017, the Law Enforcement Access to Data Stored Abroad Act and the International Communications Privacy Act, proposed by a senator, and relying on MLAT measures, failed to pass into law.
  - The key provision of the CLOUD Act amends the ECPA by requiring a provider to produce stored electronic data within the provider's "possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."
    - It applies to any information pertaining to a customer or subscriber, not just communications or other limited types of services in that it does not merely apply to emails, but also to general cloud storage.
  - Thus, the CLOUD Act provides an avenue for law enforcement agencies (LEAs) at any level, from federal agents to local police to require US organizations to provide access to user communication data regardless of where that data is stored.

The CLOUD Act of the US

- The CLOUD Act modifies the SCA by providing that the SCA's warrant authority requires "provider[s] of electronic communication service[s] or remote computing service[s]" to produce data in their custody and control, regardless of the data's location so as to clarify that it has extraterritorial effect. (CLOUD Act §§ 102, 103(a)).
  - Now US LEAs can serve a search warrant for an organization's data and the organization will have to comply, even when the data is stored in a foreign jurisdiction.
  - The CLOUD Act focuses on whether the recipient of a request has control over the data – specifically, whether there is "possession, custody, or control," as used in both US civil and criminal laws to define a party's requirement to produce evidence pursuant to a subpoena, document request, regulatory inquiry or similar.
    - The analysis of "possession, custody, and control" has different meanings in different US jurisdictions.
    - The US Second Circuit, covering the US states of Connecticut, New York and Vermont in federal matters, has one of the broadest applications of "possession, custody, and control" of all federal circuits.

The CLOUD Act of the US

- As with all federal statutes, the CLOUD Act can be applied not only to American companies, but also to foreign companies with a presence in the US.
  - A US court may exercise jurisdiction over a person or company where that entity has minimum contacts with the particular state in which the court sits.
  - These contacts may take a variety of forms, including the commission of some act within the state, contracting for the provision of goods or services within the state, or deriving some benefit from conducting business within the state.
  - They also may include the ownership of property, maintaining a bank account, or placing an item in the stream of commerce with the intention that it be distributed within the state.
  - Even if such minimum contacts with a particular state cannot be established, a federal court may gain jurisdiction over a foreign company, if to do so does not violate the requirements of due process contained in the Constitution's Fifth Amendment.
  - In conclusion, if a service provider has any significant presence in the US, it could be subject to the CLOUD Act.

The CLOUD Act of the US

- The recipient of a request provided under the CLOUD Act, i.e., a provider of electronic communication services or remote computing services, however, may ask a court to quash or modify the request if:
  - (a) the person(s) whose data is sought is not a U.S. person and does not live in the U.S.;
  - (b) compliance with the warrant conflicts with the law of the nation, i.e., a qualifying foreign governments with an executive agreement with the US, where the data are actually stored; and
  - (c) the court undertakes a comity analysis to conclude whether, on balance, disclosure is or is not warranted.
  - This process is additive, as the court must reach all three in the affirmative to quash or modify that request.
  - The law also explicitly preserves the availability of common law comity claims in those situations where the new statutory-based streamlined comity claims above are not available.
    - It may be possible for a subscriber or "middle man" (such as a bank storing its customers' data) to bring a traditional comity action, but only if it is aware of the demand in the first place.

The CLOUD Act of the US

- The CLOUD Act provides a mechanism for the US to enter an executive agreement with a foreign government that meets each of a list of privacy and human rights requirements.
  - Foreign governments are only eligible if the Attorney General, in conjunction with the Secretary of State, certifies in writing, and with an accompanying explanation, that the foreign government "affords robust substantive and procedural protections for privacy and civil liberties" with respect to relevant data collection activities.
  - Such foreign governments are required to have adopted procedures to "minimize the acquisition, retention, and dissemination of information concerning United States persons." (§105(a))
  - The statute also includes the safeguard that the agreements may not be relied upon to create a decryption mandate.
  - Any such executive agreement entered into pursuant to this provision are subject to review and disapproval by Congress.
  - The CLOUD Act also prohibits non-US law enforcement authorities from making certain document requests via the executive agreement process, including those that target a US citizen or resident. (§105(a))

The CLOUD Act of the US

- Executive agreements under the CLOUD Act allow each party reciprocal rights of access to data.
  - An Executive agreement would allow a foreign government to issue an order for electronic evidence to a provider subject to US jurisdiction where the order is (a) issued in compliance with the domestic law of that country; (b) founded on reasonable justification; (c) related to the investigation of a serious crime; and (d) targets a non-US person.
- Executive agreements are binding international agreements entered into by the executive branch, which are authorized in advance by Congress through legislation, and therefore, unlike treaties, do not require Congressional ratification.

The CLOUD Act of the US

- The CLOUD Act contains specific provisions addressing how these executive agreements will be entered into and renewed.
  - Once the Attorney General certifies a new agreement, it is to be considered by Congress.
  - The agreement will enter into force unless Congress enacts a joint resolution of disapproval within 180 days.
  - Every five years, the Attorney General is to review his or her determination that a foreign country meets the requirements for entering into a bilateral agreement.
  - If he or she renews that determination, a report is to be submitted to Congress containing the reasons for the renewal, any substantive changes to the agreement or to foreign law, and how the agreement has been implemented and what problems or controversies, if any, have arisen.

The Implications of the CLOUD Act

- The executive agreement framework of the CLOUD Act marks a substantial departure from prior practice, which requires a use of the MLA process to obtain data located in a foreign country.
  - Where a foreign country seeks data stored in the US, the MLA process requires an order to be issued by a US magistrate judge.
  - The executive agreement eliminates this *ex-ante* judicial check on foreign demands for data.
  - Many supporters of privacy and human rights resisted changes to the existing MLAT system.
- Negotiations with foreign governments over executive agreements are expected to be conducted with the US's allies.
  - The European Commission is expected to open discussions with the US on the CLOUD Act. (UK Justice and Home Affairs pre-Council statement: Written statement - HLWS1116, 5 Dec. 2018)
  - The first executive agreement under the CLOUD Act is expected between the US and the UK.

The Implications of the CLOUD Act

- When governments are forced to make a diplomatic request to the US for communications content, those content requests from governments are judged in the US under the relatively strict standard of probable cause of a crime, approved by an independent magistrate.
  - The US Government has to present "specific and articulable facts showing . . . reasonable grounds to believe that the contents or records . . . are relevant and material to an ongoing criminal investigation." (§2703(c)(2), (d))
- However, faced by an exponentially rising number of investigations seeking content of communications, other countries have been incentivized to expand data localization, which is generally against the US approach on the cross-border data flows.
  - Once data localization mandates are in place, the relatively strict US legal protections no longer apply.
  - Foreign governments can access evidence under their local law, and the US has no say as to the standards or procedures applied.

The Implications of the CLOUD Act

- As domestic and foreign laws are updated to account for the trend of data becoming increasingly not limited to geographic location, greater international harmonization is certainly necessary.
  - Without harmonization, providers can face circumstances where the law of one country requires disclosure that the law of another prohibits.
- The CLOUD Act takes a step towards harmonization through the executive agreements under its terms.
- Should countries find the CLOUD Act's requirements for executive agreements unsupportable, its legacy may work as an obstacle to rather than a useful tool for international electronic communication or storage providers.
  - As Attorney General Jeff Sessions and EU Justice Commissioner Věra Jourová met in May 2018, a momentum seems to be made towards a new EU-US solution for sharing electronic evidence for law enforcement purposes.

The Implications of the CLOUD Act

- The CLOUD Act may be criticized to restrict privacy rights by providing more government access to data.
- The CLOUD Act's compatibility with the EU's General Data Protection Regulation (GDPR) is an open question.
  - GDPR, for example, certainly forces businesses to process user data more carefully and give more rights and power to the owners of these data.
  - Some commentators note significant concerns related to data transfers under the GDPR and related CLOUD Act applications – specifically, whether executive agreements will be sufficient to address conditions set out in GDPR Arts. 44 to 50.
  - Those provisions relate to whether executive agreements could be considered "necessary for important reasons of public interest."
    - Art. 49(1) of the GDPR on derogations for specific situations states that "In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: ... (d) the transfer is necessary for important reasons of public interest;"

The Implications of the CLOUD Act

- On April 17, 2018, the European Commission published the e-evidence initiative, that would create a new framework for EU Member States to access content data and metadata (collectively "e-evidence") across national borders.
  - EU Justice Commissioner Věra Jourová said on that day, "We need to equip law enforcement authorities with 21st century methods to tackle crime, just as criminals use 21st century methods to commit crime".
  - She described law enforcement authorities' investigative methods as "cumbersome", while "criminals use fast and cutting-edge technology to operate".
  - She also said: "I want to see the EU and the US have compatible rules for obtaining evidence stored on servers located in another country, in order to solve serious crimes."

The Implications of the CLOUD Act

- The e-evidence initiative was released less than one month after the US enacted its own framework governing cross-border data access under the CLOUD Act.
- Like the CLOUD Act, the e-evidence initiative would provide new tools for law enforcement to obtain data stored across national borders for criminal investigations.
  - The proposal would enable EU law enforcement authorities to obtain data directly from providers—including providers based outside the EU—and potentially regardless of which entity in the provider's corporate structure has possession or custody over the data.
- The e-evidence initiative would suggest that the EU may be abandoning the rigid MLAT-only tool in favour of a more pragmatic approach.

The Implications of the CLOUD Act

- The e-evidence initiative thus provides support for direct EU-US negotiations under the Cloud Act in two ways.
  - First, the legal rationale for the proposed initiative supports the finding of EU competence in this area.
  - Second, any negotiations under the CLOUD Act (for the US to the EU evidence requests) would need to be closely harmonized with the e-evidence initiative/regulation (for evidence requests between EU Member States) so as to ensure harmonization of approaches across borders.

Conclusions

- The recent initiatives of the US and the EU to reinforce law enforcement access to data may be justified to combat crimes, international or domestic, or off-line or on-line.
  - The Council of Europe has been discussing to amend the Budapest Convention for "enhanced international cooperation on cybercrime and electronic evidence".
  - A Protocol to the Budapest Convention, to be adopted in this respect, may be in line with the initiatives above.
- There is to be a solid and balanced legal mechanism to protect or not to restrict privacy rights while facilitating law enforcement cooperation for combating crimes.
- .....