Андрей Ярных
Руководитель GR и стратегических проектов
Kaspersky Lab Russia

Андрей Ярных *поделился с* ***Пульсом Кибермира*** *на полях 9го Форума по информационной безопасности в Гармише-Партенкирхене своим видением трех основных проблем, отсутствие решения по которым создает значительные риски для безопасности сети Интернет.*

1. **Надгосударственный статус сети Интернет.** Это ключевой фактор и во многом первопричина существующих проблем и угроз. Интернет стал настолько значимой ценностью, что его работоспособность рассматривается странами как критически важный элемент обеспечения функционирования государства. Даже кратковременное отключение инфраструктуры может нести угрозы безопасности и обороноспособности, а в случаях связи с медициной, энергетикой, транспортом и т.д. – и прямую угрозу жизни гражданам. Оценивая риски, государства вынуждены создавать собственные дублирующие и управляющие структуры, тем самым ставя под вопрос глобальный статус сети. Сегментация глобальной сети на национальные сегменты логична с точки зрения обеспечения национального суверенитета над территориальной частью сети. Однако обособление может привести к потере возможности использования мирового опыта, совокупного научного потенциала и знаний, что повлечет отставание от глобальных структур. Решением проблемы могло бы быть признание сети Интернет «**Мировым достоянием**», открытым для изменений и совершенствования. Доступ в сеть Интернет должен стать одной из базовых ценностей человечества, обеспечивающей уровень доступа к знаниям, гарантирующим демократический уровень обмена мнениями и свободы слова. И должны быть гарантии того что эти права не могут быть ограничены по политическим или идеологическим причинам. Такой контроль над корневой

инфраструктурой сети интернет может быть обеспечен только открытым и независимым управлением, возможно под эгидой ООН или другой аналогично международной организацией (специально созданной) учитывающей и представляющей интересы всех стран. Международный, надгосударственный статус сети интернет должен обеспечить режим доверия государств и гарантировать развитие, целостность, безопасность и право равного доступа к инфраструктуре и сервисам глобальной сети Интернет.

2. **Запрет на кибер-оружие.** Это крайне опасный и в тоже время высокоточный, высокоэффективный и даже в чем-то «гуманный» вид оружия. Если альтернативой его применения является огневая военная операция, то найдется много сторонников того, что такое оружие обязательно должно быть в арсенале государств. Признавая это, все же необходимо учитывать, что такое оружие, как правило, задействует (заражает) компьютеры многочисленных гражданских пользователей сети Интернет. Такое оружие хуже поддается контролю и способно попасть в руки хакеров, радикально настроенных структур и просто террористов. Использование кибер-оружия может повлечь нарушение работоспособности и целостности сети Интернет, способно нанести реальный ущерб инфраструктуре и экономике целых стран. Обладание таким кибер-оружием способно привести **к гонке вооружений** в киберпространстве и тогда все компьютеры пользователей в сети Интернет станут потенциальными мишенями для заражения и наращивания мощности ботнет-сетей (зомби-сетей). На мой взгляд, необходим **запрет на использование кибер-оружия,** однозначное и всеобщее осуждение фактов его применения. Надгосударственная структура управления сетью Интернет может применять необходимые ограничительные меры к структурам или странам, которые используют деструктивные функции кибер-оружия и вводить ответственность за утрату контроля над его элементами, повлекшими попадание его в руки злоумышленников.

3. **Сотрудничество в расследовании трансграничных кибер-преступлений.** На уровне европейских стран была принята «Будапештская конвенция» Совета Европы (Council of Europe Convention on Cybercrime), которая содержит актуальные, на момент принятия, положения **по организации противодействия кибер-преступникам**. Однако, некоторые пункты этой конвенции, прямо указывают на возможность расследования кибер-преступлений на территории других государств, что актуально только для слабых стран, не способных самостоятельно противостоять кибер-угрозам и предпочитающих делегировать право расследования другим странам. Это оказалось неприемлемо для России, Китая и многих других стран, что привело к появлению новой инициативы по противодействию преступлениям в сети Интернет. Это будет совсем не просто, так как европейские страны в целом устраивает Будапештская конвенция, несмотря на то, что с момента ее подписания прошло уже более 12 лет. К сожалению, вопрос международного сотрудничества буксует уже много лет и это является серьезным препятствием для расследования трансграничных преступлений. В порядке экспертной помощи, Лаборатория Касперского в настоящее время осуществляет сотрудничество с Сингапурским офисом Интерпола и Европолом http://www.kaspersky.ru/about/news/business/2014/chto_obshego_u_Europola_i_Interpola_tech_KL , однако частные инициативы компаний не могут полноценно заменить государственный формат борьбы с трансграничной кибер-преступностью.