УДК 339.166:343.534(045)

Ю.Є. Муравська (Якубівська),
к.е.н.,доцент, доцент кафедри фінансово-економічної безпеки та інтелектуальної власності, Тернопільський національний економічний університет, м. Тернопіль

ТЕНДЕНЦІЇ РОЗВИТКУ ПРОМИСЛОВОГО ШПИГУНСТВА У СВІТІ

Yuliya Muravska (Yakubivska),
PhD in economics, docent, associate professor of the Department of Financial and Economic Security and Intellectual Property, Ternopil National Economic University, Ternopil

WORLD TRENDS IN INDUSTRIAL ESPIONAGE

Анотація.
В науковій статті розглянуто явище промислового шпигунства в контексті загроз для економічної безпеки підприємства, охарактеризовано парадигму розвитку явища промислового шпигунства у світі. Розглянуто тенденції розвитку промислового шпигунства на прикладі провідних світових компаній. Сформульовано висновки щодо сучасного рівня захисту від загроз промислового шпигунства на міжнародному рівні. Досліджено приклади високого рівня порушень та зловживань у процесі здійснення економічної розвідки. Акцентовано увагу на активності промислових шпигунів на ринку США та ЄС. Проаналізовано рівень фінансових збитків від промислового шпигунства. На підставі наведених положень сформовано висновки щодо низького рівня захищеності провідних компаній світу від проявів промислового шпигунства, однією з причин чого є недосконаліть системи нормативно-правового забезпечення у даній сфері. Обґрунтовано необхідність здійснення активної політики захисту від промислового шпигунства.

Summary.
The phenomenon of industrial espionage in the context of threats to economic security is considered in the scientific article; the paradigm of the phenomenon of industrial espionage in the world is described. Tendencies of industrial espionage development by the example of world's leading companies are considered. The conclusions about current level of protection against threats of industrial espionage internationally are formed. Examples of high-level violations and abuses in the process of economic intelligence are studied. The attention is focused on the activity of industrial spies in the US and EU markets. The level of financial losses from industrial espionage is analyzed. Conclusions about low level of security of leading companies in the world against the industrial

espionage are based on the formed provisions, and one of main reasons of that situation lays is imperfect legal system in this field. The necessity to implement an active policy of defense against industrial espionage is grounded.

Ключові слова. Промислове шпигунство, кібербезпека, економічна розвідка, контррозвідка, інформація, інтелектуальна власність,

Keywords. Industrial espionage, cyber security, economic intelligence, counterintelligence, information, intellectual property,

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Персональні комп'ютери стали ключовими при здійсненні промислового шпигунства через величезну кількість інформації, яку вони містять і простоту копіювання та передачі. Використання комп'ютерів для шпигунства різко зросла в XXI сторіччі. Інформація набуває розповсюдження в мережі, викрадається, копіюється з персональних комп'ютерів, що не мають паролів доступу. Ноутбуки були і залишаються головною мішенню осіб, котрі їдуть за кордон у бізнес-справах, якщо залишаються без нагляду. Аналогічна небезпека виникає при користування мережею Інтернет у готелях, де персонал має доступ до даних. Ця інформація може бути вкрадена під час перевезення, у таксі, в поїздах.

Вітчизняні компанії практично не приймають всерйоз попередження про наявні загрози в контексті порушення права інтелектуальної власності, особливо незаконних посягань на комерційні таємниці тощо. Вони копіюють чи викрадають комерційні дані, комерційну таємницю, нові технології, що при здійсненні оцінки нематеріальних активів українськими компаніями, обійдуться місцевим фірмам у значні фінансові втрати.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення не вирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Проблематика промислового шпигунства лежить в основі досліджень наступних вчених: Андерсон Н.[3], Барачіна А.[4], Браніган Т.[5], Міллер Л.[8], Чечерскі М.[6] та ін. На основі опрацювання джерел по даній тематиці прослідковується необхідність вивчення особливостей промислового шпигунства та тенденцій його розвитку в контексті визначення необхідності формування шляхів протидії зазначеному явищу. Науковці приділяють значну увагу організаційним методам захисту від промислового шпигунства. Однак поза увагою залишається економіко-правовий аналіз розрахунку втрат від промислового шпигунства,

котрий являє собою вагомий показник необхідності здійснення активної політики захисту від промислового шпигунства та заходів контррозвідувальної діяльності.

Формулювання цілей статті (постановка завдання). Основними цілями наукової статті є дослідження тенденцій виникнення та поширення загроз промислового шпигунства у розрізі країн світу, а також аналіз заходів протидії вищевказаному явищу. Задля досягнення зазначених цілей потребують вирішення наступні завдання:

- дослідити парадигму розвитку явища промислового шпигунства у світі;

- проаналізувати тенденції розвитку промислового шпигунства на прикладі провідних світових компаній;

- сформулювати висновки щодо сучасного рівня захисту від загроз промислового шпигунства на підприємствах.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Промислове шпигунство вперше було зафіксоване в Європі ще у в 1712 році, коли Франсуа Ксавьє Д'Ентреколь продемонстрував світу методи виготовлення китайської порцеляни, котрі, як вважалося, були отримані незаконним шляхом. Наступним історичним прикладом виступили взаємні звинувачення у промисловому шпигунстві між Англією і Францією у 18 сторіччі. Вони стосувалися отримання Францією таємних промислових технологій шляхом використання людських ресурсів, що були цілеспрямовано направлені на навчання в Англії, отримання відповідних знань та навичок у Шеффілді та Ньюкаслі з подальшим поверненням та використанням останніх у Франції. Даний факт призвів до формування першого англійського законодавства, спрямованого на запобігання таких методів економічного і промислового шпигунства. Під час Холодної війни у 1940-х роках між Сполученими Штатами Америки та Радянським Союзом характерним фактором став розвиток радянського промислового шпигунства, що став доповненням до інших видів шпигунської діяльності та проіснував аж до 1980-х років. Яскравим прикладом промислового шпигунства стала операція «Брунгільда», що діяла з середини 1950-х років до початку 1966 р. і використовувала шпигунів в багатьох країнах комуністичного блоку, завдяки чому багато західноєвропейських промислових секретів були скомпрометовані. Один з учасників операції «Брунгільда» Дж. Пол Соперт оприлюднив інформацію про факт промислового шпигунства, вчиненого радянською владою, врезультаті якого російські агенти отримали деталі сучасної системи електроніки «Конкорд». Крім того він дав свідчення проти двох співробітників «Kodak», котрі жили та працювали у Великобританії, згідно яких вони були звинувачені в передачі інформації про виробничі процеси на підприємстві [4, с. 133].

Ще одним об'єктом посягання врезультаті економічного та промислового шпигунства стали радянські системи спецінформації. Таємна доповідь Військово-

промислової комісії СРСР (ВПК), озвучена на протязі 1979-80 р.р., деталізує, яким чином спецінформація може бути використана в дванадцяти різних військово-промислових галузях господарства. У своїй статті Чечерскі М. докладно аналізує систему спецінформації, в якій 12 промислових галузевих міністерств сформулювали запити про надання інформації у розвитку технологічного сектора в своїх військових програмах. Отримані шпигунським методом плани були описані на два роки з розбивкою на п’ять циклів в рік і містили близько 3000 задач на кожен рік [6]. Зусилля були спрямовані на цивільні, а також військово-промислові цілі (наприклад, в нафтохімічній промисловості). Частина інформації була отримана з метою порівняння європейських рівнів конкурентоспроможності технічного прогресу та радянського. У тій же доповіді було оприлюднено велику кількість нетаємної інформації, що дало змогу не акцентувати увагу на спецінформації, а відтак не посягати на використання методів промислового шпигунства та конкурентної розвідки. Радянські військові характеризувалися значно ефективнішим використанням одержаної інформації в порівнянні з цивільною промисловістю, де впровадження нових промислових технологій було уповільненим.

У світовій практиці промислового шпигунства відомий термін «DDoS-атака». Дана комп’ютерна програма використовує злам системи комп'ютера, щоб організувати потік запитів по цільовій системі, викликаючи її закриття і відмову від доступу іншим користувачам. Дана програма потенційно може бути використана для економічного або промислового шпигунства з метою саботажу. Цей метод був використаний російськими спецслужбами, протягом двох тижнів кібератаки на Естонію в травні 2007 року у відповідь на видалення даних по воєнній епосі Радянського Союзу [3].

У попередніх дослідженнях автора [2, с. 370] запропоновано умови формування системи захисту від промислового шпигунства на макрорівні:

- формування ефективного механізму державного регулювання експорту-імпорту товарів, які містять отриману незаконним шляхом інтелектуальну власність, особливо у якості комерційної таємниці, чи виготовлені на її основі;
- податкове регулювання процесу переміщення через кордон продукції, що виготовлена або реалізовується із порушенням права інтелектуальної власності;
- гармонізація законодавства, що стосується захисту від недобросовісної конкуренції у контексті промислового шпигунства, особливо щодо питань, пов’язаних із охороною та захистом комерційної таємниці;
- стимулювання розвідувальної та контррозвідувальної діяльності у контексті боротьби з промисловим шпигунством як на національному, так і на міжнародному рівні, контроль за дотриманням чинного законодавства. У висновках до даного дослідження буде подано рекомендації щодо формування системи захисту від промислового шпигунства на мікрорівні.

Промислове шпигунство набуло свого поширення ще у минулому сторіччі, як порушення авторського та патентного права при веденні бізнесу компаніями, що здійснювали свою діяльність, використовуючи практику придбання необхідної ділової інформації та комерційних таємниць конкурентів нелегальним методом. Прикладами таких порушень виступають наступні світові компанії [9, с. 111-123]:

1. «Unilever» та «Procter & Gamble». Компанія «Procter & Gamble» зізналася в промисловому шпигунстві, яке, як стверджується, здійснювалося протягом шести місяців, та стосувалося продукції по догляду за волоссям компанії-конкурента «Unilever». Особливістю їхнього плану, який «Procter & Gamble» називає «нещасним випадком», є огляд сміття компанії «Unilever» з метою пошуку конфіденційних документів. Однак «Unilever» стверджує, що зазвичай утилізують документи в повному обсязі, а секретні, які становлять загрозу для лідера «Procter & Gamble», є пронумерованими. Компанія «Procter & Gamble» заперечує твердження журналу «Fortune» про даний інцидент. Ці компанії досягли згоди, і «Procter & Gamble» зобов'язалася не використовувати будь-яку інформацію, яку вона отримала нелегальним шляхом, в розробці свого продукту.

2. «Cadence Design Systems» та «Avant!». У пресі з'явилися звинувачення, що компанія «Avant!», що розробила програмне забезпечення для компаній Силіконової долини, вкрала код до програми конкуруючої компанії «Cadence Design Systems». Це стало яскравим випадком недобросовісної ділової практики, коли прокуратура висунула звинувачення, врезультаті чого «Avant!» була зобов'язана виплатити 182 млн. дол.. США в якості компенсацій плюс відсотки і збори, в цілому 200 мільйонів доларів США. Крім того, закриття кримінальної справи означало, що «Cadence», нарешті, зможе приступити до своєї цивільної справи. Не задовольняючись 200 млн.дол.США, «Cadence» отримана від «Avant!» угоду на придбання продукту «Synopsys» ще на 265 млн. дол США.

3. «Opel» та «Volkswagen». Негативним фактором для будь-якої компанії є перехід керівника найвищої ланки управління в іншу компанію. Прикладом цього став перехід керівника та семи його замісників компанії «Volkswagen» у компанію «Opel». Врезультаті «Opel» заявила про промислове шпигунство, а саме - за передбачувану відсутність конфіденційних документів компанії. У відповідь на це «Volkswagen» виступила із звинуваченнями в наклепі. Чотирирічна судова справа була вирішена, коли компанія «Volkswagen» погодилася заплатити «General Motors», материнській компанієї «Opel», 100 млн. дол.. США і розмістити замовлення на понад 1 мільярд доларів у вартості запчастин для автомобілів.

4. «IBM» та «Hitachi». Цей випадок промислового шпигунства, що був названий «Japscam», стосувався прав на комп'ютерні ігри. Компанія «Hitachi» таємно вступила у володіння практично повним набором «Adirondack», книг компанії «IBM». Звертає на себе увагу той факт, що в них містилася проектна документація «IBM», комерційні таємниці, що містили

позначку «Для внутрішнього користування IBM». Після тривалого судового розгляду компанія «Hitachi» заплатила «IBM» 300 млн. дол США.

5. «DuPont» та Майкл Мітчелл («Kolon Industries»). Майкл Мітчелл працював у відділі маркетингу продажів компанії «DuPont Kevlar» до моменту свого звільнення. Наступним місцем праці стала корейська компанія «Kolon Industries Inc», одна з компаній, яка виробляє волокна. Майкл Мітчелл в подальшому отримував необхідну інформацію від колег з попереднього місця працевлаштування, передаючи її корейським конкурентам. Мітчелл був засуджений до 18 місяців тюремного ув'язнення і виплати грошової компенсації компанії «DuPont» більше 180 тис.дол.США.

6. «Gillette» та Стівен Луїс Девіс. Стівен Луїс Девіс був засуджений до 27 місяців тюремного ув'язнення і виплати 1,3 мільйона доларів як компенсації за крадіжку торгових секретів від «Gillette». Девіс працював на «Right Industries», компанію, з якою «Gillette» уклала контракт, що стосувався допомогти з новою системою гоління. Девісом були відправлені конфіденційні проекти, що не співпадали з «Gillette».

7. «Microsoft» та «Oracle». Глава компанії «Oracle» здійснював прихований моніторинг за фінансуванням компанії-конкурента «Microsoft».

8. «Kodak» та Гарольд Уорден. Після завершення контракту на 30 років з «Eastman Kodak» Г.Уорден створив консалтингову компанію, інформаційна діяльність якої базувалася на конфіденційній документації, отриманій нелегальним шляхом в «Kodak». Кримінальними законодавством він був засуджений до одного року ув'язнення і штрафу в 30 тис.дол.США. Однак за підсумками аналітиків, оціночна вартість викраденої інформації «Kodak» становить мільйони доларів.

9. «Starwood» та «Hilton». Компанія «Starwood» звинуватила конкурента «Hilton» у промисловому шпигунстві. «Starwood» акцентувала на ідеї люксового бренду, ідея якого була викрадена працівниками під час перевезення конфіденційної документації. Компанія «Hilton» була зобов’язана здійснити платежі на користь «Starwood», а також утримуватися від розробки конкуруючих брендів розкішних готелів на протязі трьох років від дати інциденту.

10. «Google» та операція «Aurora». Компанія «Google» оголосила, що оператори з території Китаю здійснили крадіжку інтелектуальної власності, зокрема, облікових записів електронної пошти від захисників прав людини. Керівники «Google» зазначили, що даний злочин був частиною більш широкої кібератаки від компанії в Китаї, яка стала відома як операція «Aurora». Зловмисники розпочали кібернапад, використовуючи незахищеність браузера Microsoft Internet Explorer, запустивши нову модифікацію трояна «Hydraq». Існувало припущення, що серед «інсайдерів», котрі брали участь у кібернападі, значна частина співробітників Google China, яким було відмовлено в доступі до внутрішніх мереж

компанії. Через місяць комп'ютерні експерти американського Національного агентства безпеки ствердили, що атаки на «Google» походили від двох китайських університетів, чия спеціалізація пов’язана з галузями комп'ютерних наук: «Shanghai Jiao Tong University» та «Shandong Lanxiang Vocational School», останній з котрих має тісні зв'язки з китайською військовою сферою. Деякі коментатори стверджували, що кібернапад був частиною узгодженого китайського промислового шпигунства, спрямованого на отримання високотехнологічної інформації для стимулювання економіки Китаю. Критики вказували на той факт, що ставленням до інтелектуальної власності іноземних компаній в Китаї є зневажливим, оскільки керівництво таких компаній намагається копіювати або перепроектовувати технології. Через місяць компанія «Google» вирішила припинити діяльність по високотехнологічному сектору в Китаї, що призвело до закриття операції «Aurora» [5].

На фоні процвітаючого промислового шпигунства необхідним є ефективне урядове втручання, що є неможливим без гармонізованого впливу законодавчої баз на дані процеси. Проблеми національних урядів високорозвинутих країн світу вкотре показують недосконаліть розвитку останньої.

У доповіді до уряду США від компанії «Northrop Grumman», що здійснює діяльність в аерокосмічній та оборонній галузях, подано твердження, що стосується китайського економічного шпигунства, яке становить «єдину найбільшу загрозу для технологій США». Звертання полягає у необхідності захисту інформації, що стосується досліджень та розробок, а також обсягів та джерел фінансування від китайських конкурентів [7, с. 16]. Побоювання з приводу масштабів кібератаки на Сполучені Штати Америки, котрі походять з Китаю, призвели до ситуації у сфері порушення права інтелектуальної власності, котра отримала дефініцію «нова холодна кібервійна». За даними Американського товариства промислової безпеки (ASIS), випадки промислового шпигунства в американському бізнесі виросли на сьогоднішній день більш ніж на 260 % з 1985 року.

Ще однією країною, що активно бореться з промисловим шпигунством, є Великобританія. Керівник компанії «MI5» розіслав конфіденційні листи 300 керівникам та відділам безпеки банків, бухгалтерам та юристам із попередженням щодо загрози атаки від китайських урядових організацій. Загальна інформація була також розміщена на захищеному веб-сайті Центру по захисту національної інфраструктури, доступ до якого мали компанії «критичної інфраструктури», включаючи телекомунікаційні фірми, банки і компанії водопостачання та електрики. Попередження містило дані про запуск вірусів «троян», а також програмного забезпечення, спеціально призначеного для злому конкретної фірми і витягу даних. У той же час Китай був ідентифікований як країна, що є найбільш активною у використанні інтернет-шпигунства. Китайський уряд відповів Великобританії на

звинувачення в економічному шпигунстві, твердженням, що доповідь щодо такого роду діяльності була «наклепницькою», а уряд Китаю виступає проти зломів та кібератак, які заборонені законом [5].

За підрахунками експертів, французька економіка, втрачає щорічно близько 53 млрд. євро, що еквівалентно 30000 робочим місцям по причині економічного шпигунства [8, с. 272]. Основними виконавцями вважаються Китай та Росія, з різними використовуваними у шпигунстві методами: від шпигунства, підслуховування телефонних розмов і крадіжки ноутбуків, до інтернет-атак, використання вірусів «Trojan», по електронній пошті. Метою цих атак є отримання не тільки інформації про технології, але і методів управління і маркетингових стратегій, доступ до інтелектуальної власності в режимі он-лайн спонсорованими державою хакерами. У одному з попередніх досліджень автора [1, с.159] проаналізовано заходи, завдяки яким уряди високорозвинутих країн світу ведуть активну боротьбу з промисловим шпигунством, а саме: впроваджують використання різного роду кодів доступу до інформації, захищають комерційні таємниці, перевіряють працівників підприємств, рекомендують підписання договорів про нерозголошення конфіденційної інформації, фінансово підтримують високотехнологічний сектор, акцентують увагу на стратегічному управлінні у воєнній та оборонній сферах.

Для України корисним є досвід розвинутих країн світу, що вже тривалий час працюють над вирішенням проблеми промислового шпигунства як на національному, так і при виході на міжнародний ринок. Адже відомо багато прикладів порушення права інтелектуальної власності в контексті посягання на фінансово-економічну безпеку. Зазвичай, відомі світові компанії діють по відповідній схемі, що має своїм результатом порушення законодавства.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Тенденції промислового шпигунства, які розглянуті у даній науковій статті, символізують про необхідність здійснення активних заходів захисту від проявів промислового шпигунства, а саме:

1. Визначити, яка інформація є чутливою і класифікувати її як таку. Інформація про дослідження та розвиток, процеси та інновації або нові ринкові стратегії легко ідентифікується як «вразлива». Проте, така інформація, як особисті справи, структура цін, а також бази клієнтів часто залишається незахищеною.
2. Провести оцінку ризиків з метою виявлення вразливостей, а також розрахувати ймовірність того, що третя особа може використовувати ці вразливості і отримати доступ до конфіденційної інформації.
3. Встановити, проаналізувати і оновлювати політику безпеки на підприємстві та сформувати відповідні гарантії, як процедурно, так і технологічно, щоб зірвати спроби використання уразливостей і отримання доступу до цінних даних компанії третіми особами.

4. Забезпечити надійність персоналу. Користувачі, менеджери і IT-фахівці повинні бути попереджені про те, що інформація про бізнес повинна бути захищеною, а методи, які можуть бути використані для отримання доступу до конфіденційних даних, повинні бути виявлені вчасно та нейтралізовані.

Список літератури.

1. Якубівська Ю. Є. Вплив промислового шпигунства на сферу інтелектуальної власності / Ю. Є. Якубівська // Зовнішня торгівля: економіка, фінанси, право : Науковий журнал. - К. : УДУФМТ, 2013. - № 4 (69). - С. 158-162.

2. Якубівська Ю. Є. Цільові атаки в контексті промислового шпигунства / Ю. Є. Якубівська // Проблемы развития внешнеэкономических связей и привлечения иностранных инвестиций: региональный аспект: сб. науч. тр. – Донецк : ДонНУ, 2014. – Т. 2. - С. 368-372.

3. Anderson N. Massive DDoS attacks target Estonia; Russia accused : [Електронний ресурс] / Nate Anderson // Ars Technica. Retrieved, 2016. – Режим доступу: http://arstechnica.com/security/2016/05/massive-ddos-attacks-target-estonia-russia-accused, (Accessed 27 December 2016)

4. Barrachina, Alex and Tauman, Yair. Entry and espionage with noisy signals: Games and economic behavior: Elsevier. - 2014. - N 83. - p. 127-146.

5. Branigan T. Google to end censorship in China over cyber attacks : [Електронний ресурс] / Tania Branigan // The Guardian. Retrieved, 2016. - Режим доступу: http://www.guardian.co.uk/technology/2010/jan/12/google-china-ends-censorship, (Accessed 27 December 2016)

6. Ciecierski, Marek. Szpiegostwo przemysłowe opanowało cyberprzestrzeń [Electronic resourse] / InteriaBiznes: 2016. - Access: http://biznes.interia.pl/wiadomosci/news/szpiegostwo-przemyslowe-opanowalo-cyberprzestrzen, (Accessed 27 December 2016)

7. Everett, Bernet. Optically transparent: the rise of industrial espionage and statesponsored hacking: Feature, InfoGuard. - 2016. - p. 13-17.

8. Miller, Lesley Ellis. Innovation and Industrial Espionage in France: An Investigation of the Selling of Silks through Samples: Journal of Design History. - 2015. - Vol. 12, No. 3. - p. 271-292.

9. Wright P. Spycatcher. New York / Peter Wright // Viking, 2015. - 270 p.

References.

1. Yakubivska, Y.Ye. (2013), “The influence of industrial espionage on the intellectual property sphere”, *Zovnishnya torgIvlya: ekonomIka, fInansi, pravo*, vol. 4 (69), pp. 158-162.

2. Yakubivska, Y.Ye. (2014), "Target attacks in the context of industrial espionage", *Problemyi razvitiya vneshneekonomicheskih svyazey i privlecheniya inostrannyih investitsiy: regionalnyiy aspekt*, vol. 2, pp. 368-372.

3. Anderson, N. (2016), "Massive DDoS attacks target Estonia; Russia accused", *Ars Technica. Retrieved*, [Online], available at: http://arstechnica.com/security/2016/05/massive-ddos-attacks-target-estonia-russia-accused, (Accessed 27 December 2016)

4. Barrachina, A. and Tauman, Y. (2014), "Entry and espionage with noisy signals: Games and economic behavior", *Elsevier*, vol. 83, pp. 127-146.

5. Branigan, T. (2016), "Google to end censorship in China over cyber attacks", *The Guardian*. [Online], available at: http://www.guardian.co.uk/technology/2016/jan/12/google-china-ends-censorship, (Accessed 27 December 2016)

6. Ciecierski, M. (2016), "Szpiegostwo przemysłowe opanowało cyberprzestrzeń", *InteriaBiznes*, [Online], available at:: http://biznes.interia.pl/wiadomosci/news/szpiegostwo-przemyslowe-opanowalo-cyberprzestrzen, (Accessed 27 December 2016)

7. Everett, B. (2016), "Optically transparent: the rise of industrial espionage and statesponsored hacking", *Feature, InfoGuard*, pp. 13-17.

8. Miller, L. E. (2015), "Innovation and Industrial Espionage in France: An Investigation of the Selling of Silks through Samples", *Journal of Design History*, vol. 12, No. 3, pp. 271-292.

9. Wright, P. (2015), "*Spycatcher"*, Viking, New York, USA.